VENONA

I. INTRODUCTION

A. Problems of Terminology

This historical study carries a burden of anachronistic terminology, starting with the key word in the title—VENONA. The term Venona only came into use in the 1960s, the fourth, depending how one counts, codename for the US–UK exploitation of high grade Soviet intelligence service communications. Furthermore, the most spectacular breakthroughs occurred before a codename was regularly put on product reports of this type. The term Classical [redacted] (for Russian Diplomatic) might be preferred, but Venona has now widely appeared in open sources. Then we have the problem of organizational designators for both sides, and now even the matter of naming the opposition country. The term Venona will generally be used with the earlier codenames introduced if required by the context e.g. for quotations from US–UK documents. Those earlier codenames were: JADE, BRIDE and DRUG.

KGB and GRU will be the exclusive designators for the opposition services—the entities whose communications we exploited—except that NKVD will be used when the reference is to the militarized or police elements of the state security apparatus.

For our side the matter of organizational designators is more difficult, because we devote a great deal of attention to the very early years of the Russian problem, taking care to describe in some detail who did what, when. Therefore, the contemporary and often changing names for the U.S. organizations will sometimes be used.

B. Venona

Venona is the most recent code name for the US–UK exploitation of encrypted KGB and GRU communications of the period 1941–48. Except for one lane, Canberra—Moscow, none of the traffic was read until long after the messages had been sent. Venona was not a real-time or near real-time operation. New York KGB messages of, for example, 1944 or 1945 were not first read until December 1946 (one message) and 1947. The greatest period of decryption and translation, at least for KGB messages on the U.S.—Moscow lanes, occurred in 1948-mid 1950s, and mostly involved KGB messages sent in 1944 and 1945. As we will describe, the Venona exploitation program ran until September 1980, the last published translation being a KGB message that had been sent in 1943.

Several points made here will be built upon and repeated throughout the study.

For many years the ASA–AFSA–NSA cryptanalysts worked the Russian Diplomatic problem as a whole, attacking both current messages and accumulated back traffic. The material that came to be known as Venona, imbedded in that Diplomatic traffic, comprised only a small minority of the whole. Trade messages—ultimately designated as [redacted]—were highest in volume. These Trade communications, sent in diplomatic channels, concerned Lend Lease information and reports to and from the Soviet Government Purchasing Commission: an immense volume of information about equipment, parts and other supplies needed by and being sent to Russia to assist in the war against Nazi Germany. True Diplomatic, essentially Consular messages, later called [redacted] passed between the US–UK and the Soviet Foreign Ministry. What we know as Venona also passed on Diplomatic links:

I. INTRODUCTION

- KGB (known to US–UK as [redacted] or [redacted]
- GRU (known as [redacted] or [redacted]
- GRU-naval (known as [redacted] or [redacted]

The Trade messages bore the address of the Trade Ministry; all the other systems, including the intelligence service messages, that of the Foreign Ministry, or at the US–UK end, the embassy or consulate. The true identity of the communicants was concealed by cipher. Each Russian entity had its own unique codebook. In attacking all these systems simultaneously, the US–UK followed two points of doctrine, the first an absolute cryptanalytic necessity, the second a matter of cryptanalytic optimism:

- First, from the similarities of cryptographic indicators and other message externals, it became clear early on that all classes of so-called Russian Dip should be worked together to find the best messages to attack. As we shall see from the results obtained, if a cipher pad used for routine Trade messages could be matched with an identical cipher pad used by the KGB, then a so-called "depth of two" existed and the messages might be read. (The actual text of the Trade message would be of no interest.)

- Second, the UK and the US had had tremendous, virtually 100% success against German and Japanese high grade ciphers, both machine and manual, during World War II—the German Enigma and the Japanese Purple machines for example. The U.S. had even broken a German diplomatic one–time pad system. Our cryptanalysts therefore remained optimistic that high grade Russian diplomatic systems (and military) would also fall. For that reason [redacted] Many of the high level military systems were entered fairly quickly as we had hoped—and then lost quickly because of probable espionage at ASA (a case we will discuss at length).

The Venona project, then, remained frozen in time. Russian traffic of 1942 to 1946 (rather little on each end) could be exploited but that was all. The Venona cryptanalyst of 1948 could read KGB messages of 1944; in 1980, the Venona cryptanalyst was still exploiting that same block of exploitable traffic that had been sent in the 1940s. But if the US–UK analysts [redacted] the Russians couldn't very well get back the earlier traffic that could be exploited. They had to wait—or make emergency moves as in the case of Burgess and Maclean—as their spies were identified.

A few words on Russian cryptographic systems and myths relating to them. The Venona traffic passed on both international commercial radio circuits and national links. The communications were encrypted by first using the values in a code book and then enciphering those numbers from one–time pads, that is, by taking the numbers from the pads and adding them to the numbers from the code book. Such a system could not be broken unless the cryptanalyst possessed the one–time pads (of which there were hundreds of thousands) or knew the precise means of pad generation (that is, how the numbers in the pad had been selected) and could replicate it. A third possibility remained: the key in the pads might be somehow misused or re-used and thus lose their uniqueness. That was our opening into Venona.

As for the myths, the so-called "Black Friday", 20 December 1949 was not a Friday, and is an event of no real significance to the US–UK cryptanalytic effort on Venona or Venona related materials. Likewise the Venona breakthrough did not come about because the OSS had obtained Russian codebooks. The OSS did not in any way contribute to the Venona break; the fundamental cryptanalytic discoveries and the decryptions through 1952 were not aided by our side having any KGB or GRU code book from any source. It was an analytic success. The story of the capture of Russian cryptographic material is an interesting one and will be told in some detail. But the benefits from those actions came later in the Venona story (and to repeat, had nothing to do with the OSS).

C. Scope of this Study and Sources

Much of this study will be non–technical. However, significant technical information will make unannounced appearances throughout the text, written by Cecil Phillips, one of the founders of the Venona program.

In the course of this study, the term "I" usually refers to Benson, the principal author of the study; and "we" may refer to Benson and Phillips or merely the form suggesting a partnership between author and reader.

The study contains three major themes, or perhaps we should say, the histories of three different aspects of Venona:

1. U.S. exploitation of the Venona material, at ASA, AFSA and NSA, with emphasis on the earlier years (1943–1954) but including the entry of the FBI, CIA and GCHQ onto the problem.

2. KGB and GRU espionage, tradecraft and special activities in the U.S. (and Mexico) as revealed in the Venona decrypts—case studies, examples.

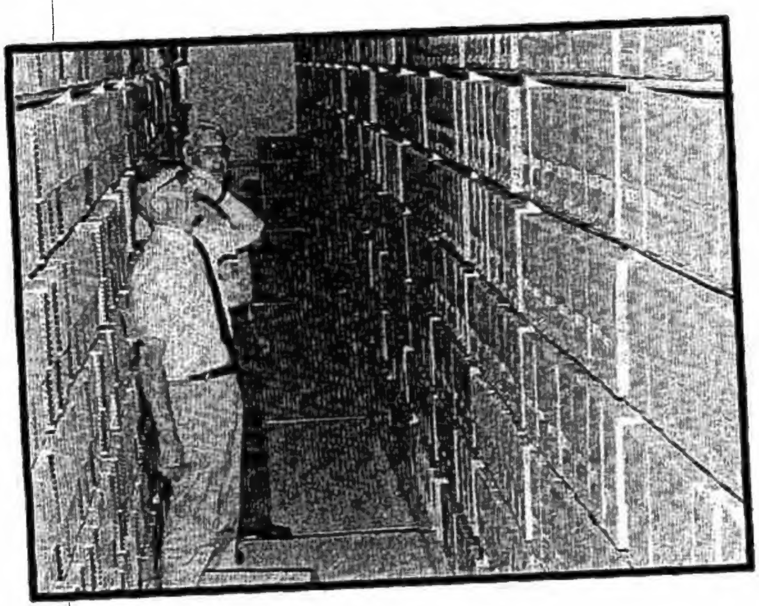
3. KGB espionage against the Venona effort.

This study emphasizes the U.S. Venona experience, but with, I hope, considerable attention to the fact that Venona exploitation became a US–UK partnership. This study would have been difficult to write without the UK documentary sources held in the NSA Venona collection. [redacted]

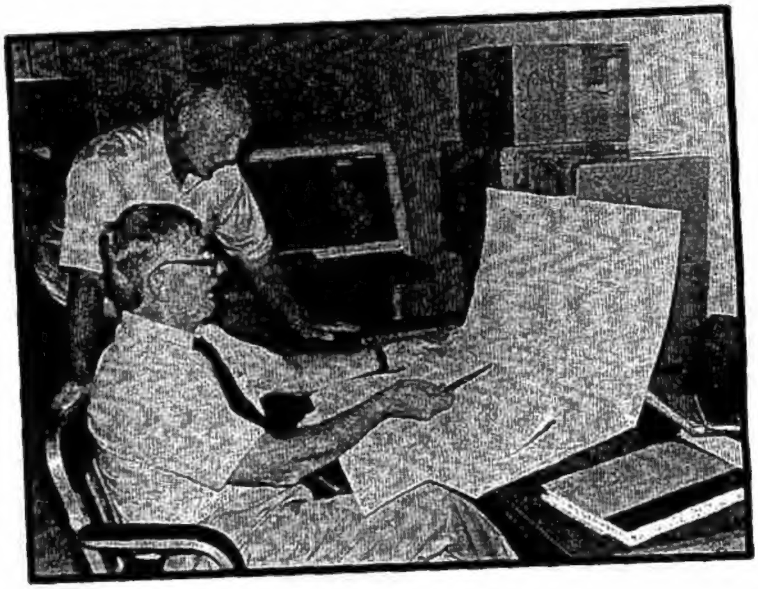
This study should be considered a source book. It is not the history of U.S. counterintelligence or Russian espionage. Often, usually in fact, I have not put a case in full context—we are after the Venona part of the record, often to the exclusion of the rest of the story. On the other hand, I have in some cases gone rather far afield. Sometimes this is a matter of preference.

In authorizing, and indeed commissioning this study, Bill Crowell, as NSA Chief of Staff and then DDO, said it was time that we put together the NSA view of Venona, to have on the shelf, ready to take out and show to the appropriate audience, the story of an exceptional undertaking by this agency and its predecessors.

I. INTRODUCTION



◀ Cecil Phillips (foreground) and Lou Benson in the Venona Collection.



Cecil Phillips and Bill Hawkins examining a Venona cryptanalytic worksheet. ▶

EXEMPT

D. Sources

The sources for this study include four major archival collections:

1. The Venona Collection. Held in the NSA archives and records center, having been preserved and sent there by Mildred Hayes, and then inventoried and protected by Bill Hawkins, this is the most important the [redacted] collection: the four boxes of Venona translations, the 700,000 messages held in 1391 Shinn boxes, the cryptanalytic worksheets and the 200 boxes of everything else: FBI and CIA reports, logs, code books, TICOM

material, technical reports, GCHQ papers, correspondence and etc. (note the amount of material that went into the production of just four boxes of translations).

2. The NSA Archives. This was a major source for early papers on the Russian problem, TICOM papers, and for organization charts and photographs.

3. The archives of the NSA Center for Cryptologic History. Again a major source for the early history of the Russian problem, containing papers of exceptional interest and importance such as the Sam Snyder diaries and the many volume history of the SSA (The U.S. Army's Signal Security Agency).

4. Counterintelligence papers of the NSA Office of Security.

Cecil Phillips and I, jointly or independently, conducted many interviews of Venona veterans including the two people who started the Russian problem in 1943 and the person who turned out the lights on Venona in 1980. I conducted a number of interviews at GCHQ, and interviewed UK Venona veterans visiting the U.S.

On occasion I do not cite a source when it might seem appropriate, and a few times the source seems to have been obscured. This is intentional.

(THIS PAGE INTENTIONALLY LEFT BLANK)

II. THE BEGINNING OF THE RUSSIAN PROBLEM, FEB–DEC 1943

Gene Grabeel, who founded the U.S. Russian Sigint program on 1 Feb 1943 (1942 photo).

II. THE BEGINNING OF THE RUSSIAN PROBLEM, FEB–DEC 1943

A. February 1943

The Russian Sigint problem began on Monday, 1 Feb 1943, in great secrecy and with minimum resources — just two people, Miss Gene Grabeel and 2/Lt Leonard M. Zubko, both recent arrivals at the Army Signal Security Agency, Arlington Hall Station, Virginia. Lt. Zubko, a 1942 graduate of Rutgers University (BSME) came to Arlington Hall after completing the Infantry School at Ft. Benning. He did not know what to expect and had never heard of the place. As a combat arms officer anxious to command troops, he was surprised to find that Arlington Hall seemed to be staffed entirely by female civilians.[1] Though he never knew for sure, he assumes that he got the assignment to Arlington Hall because he was an engineer, and the Russian assignment, several months later, because he knew the language (his parents had come from the Ukraine).

Gene Grabeel's assignment to the Russian problem was even more unlikely. After graduating from Longwood College in Farmville, Virginia, she taught at the high school in Madison Heights, near Lynchburg, Virginia. She did not like teaching. In Fall 1942 (in her second year as a schoolteacher) she asked her father what he thought about her taking a job with the federal government. He encouraged her to "go to Washington for six months and shuffle papers." In early December she talked to Lt. Paavo Carlson, a young Signal Corps officer who was recruiting civilians at the Post Office in Lynchburg. He offered her a position with the Army in the Washington area, but would not tell her what she would be doing. He asked her to leave for Washington the next day. Miss Grabeel accepted the position but told Lt. Carlson that she needed a little time to find a replacement teacher. On Sunday, 28 December 1942, she arrived in Washington, took a taxi to Arlington Hall and reported to the duty officer. Four weeks later she and Lt. Zubko started the Russian problem.[2]

Major Frank Rowlett, a friend and neighbor of her family in Virginia, and a senior officer at Arlington Hall, took her to meet Lt. Zubko. Rowlett told them to observe the strictest secrecy, and not to discuss their project with co-workers. Otherwise she received no particular instructions on how to begin or anything about the nature of the target.

Miss Grabeel and Lt. Zubko went to work. They sat at two tables in one corner of a room, the only other occupant being Major Geoffrey Stevens, the British liaison officer at Arlington Hall who had a desk in another corner. This curious and perhaps accidental arrangement may have led to some difficulties, for at that time and indeed for the next two years, the Army did not share with the British even the "fact of" the U.S. Sigint effort against Russia. Miss Grabeel and Lt. Zubko began by sorting back traffic by lane and date, looking for ways to categorize the material by system and user. Arlington Hall held a considerable body of Russian traffic (variously estimated as several or 6 to 8 filing cabinets full), and as the matter of coverage and the search for back traffic forms a significant part of the Venona story, we now consider what was available to the U.S. up to Feb 1943.

B. The Traffic

The Signal Security Agency's predecessor organization, the Signal Intelligence Service, acquired a dedicated intercept unit in Jan 1939, namely the Second Signal Service Company (later battalion) which operated several monitoring stations (MS) in the pre-war period including:

[1] Zubko, telephone conversation, 18 March 1992. The Signal Security Agency, re-named the Army Security Agency in 1945, eventually employed more than 5000 women. The women employees worked a wide range of duties, from clerical to crypto-linguist. WAC enlisted personnel had a major role in intercept operations, especially at the SSA field site at Two Rock Ranch, California, the principal site for the collection of Japanese Army mainline traffic.

[2] Grabeel interviews, 15 Oct 1991 and 10 March 1992 at Blackstone, Virginia; first interview by Robert L. Benson, second by Benson and Cecil Phillips. Carlson did not recall recruiting Miss Grabeel but has vivid memories of the recruiting campaign.

MS–1 Ft. Monmouth, NJ

MS–2 The Presidio of San Francisco

MS–3 Fort Sam Houston, Texas

MS–4 Quarry Heights, Canal Zone

MS–5 Fort Shafter, Hawaii

MS–6 Fort McKinley, Philippine Islands

MS–7 Fort Hunt, Virginia

These were fairly modest operations, for example, the Fort Sam Houston operation staffed by 11 enlisted men; the Fort Hunt site by one officer and 25 enlisted men (these are sample figures from 1939–41; the numbers and sites changed from time to time). Before establishing the Second Signal Service Company, the Army had relied on various other ad-hoc and often changing intercept arrangements. For example, in an early experimental operation—a hearability study and traffic sampling—the Provisional Radio Intelligence Detachment at Ft. Monmouth, commanded by Lt. Mark Rhoads, logged 381 foreign diplomatic messages from 1 Oct 1933 to 1 July 1934, including 63 Russian diplomatic messages.[3] Regular U.S. intercept of Russian diplomatic traffic, which contained KGB and GRU communications (though of course this was unknown to the U.S. at the time) began in 1939 as part of a general effort against all or most foreign diplomatic communications passed on international commercial circuits. The Army Signal Intelligence Service did not attempt a cryptanalytic attack on the Russian traffic but put it aside for future study.[4]

However, at the risk of pushing this study ever further back in time and away from Venona, we must note that during the 1920s and up to 1932, the Signal Intelligence Service had unsuccessfully attempted to break Russian diplomatic systems. The major effort took place in 1930–31 when Congressman Hamilton Fish, as chairman of the House Committee on the Investigation of Communist Propaganda, subpoenaed copies of Amtorg Trading Corporation messages held by U.S. cable and telegraph companies. He turned these over to the Navy for analysis and the Navy, unable to break into the messages, passed them along to the Army. No luck there either. It is worth quoting some comments made to G–2 in Feb 1931, by Major D.M. Crawford, head of the Signal Intelligence Service:[5]

> *Judging by what is known of Russian cryptographic methods in general, the (Russians) are employing complicated, scientifically constructed systems designed to resist the organized efforts of expert cryptanalysts. It is my belief that half-way measures and sporadic attempts will get nowhere in this case; nothing short of deep, long continued, and painstaking analysis has any chance of leading to a successful solution.*

The Venona story indeed!

While U.S. cryptanalytic and translation resources had to be concentrated on the highest national priorities of the time—Japan, Germany and Italy—collection procedures allowed for a vacuuming up approach. From 1939 to 7 December 1941, we find that encrypted Russian diplomatic traffic was taken in a modest amount from two principal sources: intercept of commercial circuits (that is foreign government traffic sent and received by, for example, RCA), by Station 3 at Fort Sam Houston — which seems to have had the principal responsibility

[3] "History of SSA in World War II", Volume XIII, Part I, 1945. Center for Cryptologic History (CCH), IV.B.1.13

[4] Interview of Frank B. Rowlett, by Benson, 14 Jan 1992, Sarasota, Florida.

[5] "Data on Soviet Cryptographic Systems 1917–33", Signal Security Agency, 15 May 1945. CCH Collection, III.O.22. See especially pages 14–15.

for copying the Russian traffic; and clandestine photography of Russian messages filed at the U.S. cable companies.

The clandestine photography procedure originated in an arrangement between the Army Signal Corps and David Sarnoff, chief executive officer of RCA and a reserve Signal Corps officer. In January 1940, Mr. Sarnoff wrote the Adjutant General accepting a War Department proposal to have a Signal Corps officer assigned to RCA for six months, "to pursue a course of study." As Earle F. Cook (Major General, retired) would recall "All of this nonsense was a cover — looking over the traffic was what I was there for."[6] With the cooperation of RCA, who provided a safe room and photo equipment, diplomatic messages were photographed and delivered to the Signal Intelligence Service. While Cook describes the Washington DC operation in some detail, we know that similar photo operations took place in New York City and possibly San Francisco. Photography meant perfect copy of the message as sent and allowed coverage of traffic that had not been intercepted or could not be (the Army copied manual and high speed morse but not printer).

Earle F. Cook. "Looking over the traffic was what I was there for"

A sampling of KGB (and some GRU) traffic from 1940 until 7 Dec 1941 on U.S.<—> Moscow lanes shows that both intercept and photography were extensive, but the coverage erratic. KGB New York traffic was intercepted by Station 3, mostly, but also by Stations 4 and 7 (Canal Zone and Fort Hunt, VA respectively) throughout 1941, while the photography mostly took place in January and again during the last few months of that year. Washington <—> Moscow GRU was collected by both means, especially for January–August 1941. Only a small amount of Russian intelligence traffic to and from San Francisco and Los Angeles seems to have been taken. The KGB did not communicate out of Washington until 1943 (the New York City Residency serviced the KGB station in Washington).

The KGB and GRU traffic represented a minority of the Russian messages sent and collected — the bulk of the material then and later would be Trade and Consular.

[6] NSA interview of General Cook, 15 July 1982, by Robert D. Farley, OH 14–82, CCH Collection. See also the interview of Colonel Robert E. Schukraft, 2 Oct 1980 by Bob Farley, OH 36–80. These interviews are extraordinary sources of information about Army Sigint.

The Army and Navy discussed the collection and processing of Russian traffic in some of their pre-war negotiations on coordination. From July–Oct 1940 several committees met to discuss a division of overall U.S. intercept effort, especially of diplomatic communications. The Army, or at least General Mauborgne, the Chief Signal Officer, preferred to divide the intercept coverage based on the transmitting station. The Navy preferred a more comprehensive scheme based in part on target entity, but eventually agreed to the Army proposal, though with the interesting proviso that the Army would turn over to the Navy all Russian traffic.[7] A small Navy effort against Russian diplomatic, begun in 1938 and which perhaps continued into 1941, produced no results and did not influence later work on this target.[8]

On 7 December 1941, the U.S. established censorship of international mail and communications. This should have given the Signal Intelligence Service all Russian traffic on the U.S.<—> Moscow lanes, as the cable companies were now required to turn over to the Censor a copy of every communication. The Venona traffic files contain Censorship copies of KGB traffic (N.Y.<—> Moscow) starting on 16 December. The early censorship coverage seems to have been quite complete, but then, unaccountably, the coverage drops off and from the end of Jan 1942 until mid-May, and for other short periods during 1942, significant gaps exist. In other words some hundreds of KGB and GRU messages from 1942 are missing and presumably were not taken from any source (that is, intercept and photography were cut back in favor of the seemingly more certain censorship source — so everyone dropped the coverage). The Army continued to intercept some Russian diplomatic on the non–U.S. lanes, such as Moscow <—> Tokyo. While 1942 KGB traffic is less likely to be readable than that of 1943 to 1945 (and GRU even less readable for 1942), the cryptanalytic success rate would presumably have increased had all the messages been available.[9]

By later 1942, censorship coverage had improved with nearly complete coverage on the U.S.<—> Moscow lanes. In summary then, on 1 Feb 1943, Miss Grabeel and Lt. Zubko had an extensive and ever-growing body of Russian traffic to work with, some dating back to 1939 (very little 1939 traffic has survived). Yet this certainly represented much less than half of what had been passed in those years.

C. Interlude: The Sinkov Mission to the UK

The United States entered into a de facto but limited Sigint arrangement with Britain in 1940, beginning with some discussions in London between the British Naval Intelligence Division and the U.S. Naval Attache. This came to nothing but in August 1940, a high level Army–Navy delegation went to the U.K. to evaluate British ability to continue the war. One of the American visitors, Brigadier General George V. Strong of the General Staff (and later Assistant Chief of Staff, G–2) told the British that the U.S. had solved the Japanese Purple (diplomatic) machine cipher. Strong then radioed General Marshall suggesting a formal exchange program for German, Japanese and Italian Sigint information. In Feb 1941, a U.S. mission went to GCHQ (sailing to England on the Royal Navy battleship <u>George V</u> which they had boarded at Annapolis). The party consisted of Captain Abraham Sinkov and 1/Lt Leo Rosen of the Signal Intelligence Service and Robert Weeks and Prescott Currier from the Navy's OP–20–G. The main purpose of the mission was to exchange information

[7] See "Catalog of Papers", Volume I, a collection prepared by AFSA in 1952 and held by the CCH. My summary of these negotiations is based on my notes from some earlier research.

[8] The Navy's lack of success on the Russian diplomatic target can be inferred from later Army—Navy discussions and the Navy's own summary of its work on Russian communications which reported no significant effort until the summer of 1943. Colonel Schukraft confirmed that the Army gave the Navy copies of all Russian intercept in the pre-war era , "because they were working on it. They told us they were."

[9] We surveyed the traffic logs and the boxes of actual traffic held in the Venona collection. Gloria Forbes, who joined SSA in 1943 and worked in the traffic section recalled that a significant gap existed in censorship coverage for 1942. (Interview by Benson and Phillips on 18 Dec 1991).

and material on the Axis powers (the British got Purple, the Americans learned a little about the Enigma break). The British gave Capt. Sinkov the following information about Russian systems:[10]

- Details of the Russian weather ciphers
- Information about OKK 5 and OKK 6, major Russian army and air force systems
- An NKVD air system
- Russian call-sign and radio procedure (army, air and NKVD/police)

In a hand-written note to his summary report on Russian systems, Sinkov concluded, "The Russian secret systems utilize a one part code book. These code books are super enciphered using additive, or special tables which vary from day to day."

Sinkov's report does not specifically mention Russian diplomatic or intelligence service systems or anything about the extent of British coverage of the Russian target. The British as we will see would soon make some important decisions about their coverage of Russian targets.

The British had obtained some Russian military codebooks and other cryptographic material from the Finns during the Winter War of 1939–1940 (the First Russo Finnish War) when Colonel John Tiltman, a senior GCHQ officer had visited the Finns to discuss Sigint collaboration. These codebooks represent a different trove than the so-called Petsamo material. The Petsamo cryptomaterial, which included a KGB codebook, instructions for using additive, tables and an emergency cipher system, came into Finnish hands in June 1941 at the start of the Second Russo Finnish War, reached the Swedes in 1944, and UK–US in 1945–46. We will discuss that in some detail later in this study.

D. <u>The Decision to Begin the Russian Problem</u>

Though putting two very junior analysts in a room on 1 Feb 1943 seems a small investment in resources, it represented a significant political decision considering the climate of the times and the considerable sympathy and admiration for wartime Russia held by many Americans. Unfortunately, we can find no date of decision and no policy papers that clearly relate to the decision. Frank Rowlett, one of the senior officers of the Signal Security Agency and later a senior official at NSA says that the decision to open the Russian problem was more or less inevitable considering the Army Sigint doctrine of the time.[11] That doctrine had come from Colonel Carter W. Clarke, Deputy Chief of the Military Intelligence Service (an operating agency of the G–2, Army General Staff) and head of the Special Branch. Clarke told Arlington Hall that in spite of the need to give maximum intelligence support to the war against Japan and Germany, Sigint collection against all other actual or potentially important targets must continue. That meant the Army was not to drop general diplomatic collection and should expand its cryptanalytic effort against those targets.

Clarke, a career Signal Corps officer who had been assigned to G–2 in 1941 (originally to head counterespionage) broadly controlled the Army's national Sigint programs and policies throughout the war and

[10] Sinkov report, undated but 1941, CCH Collection IV.v.7.5

[11] Rowlett interview by Benson, Orlando, Florida, 14 Jan 1992.

well into the Venona period[12] A sample of Clarke's thinking on Sigint policy can be found in his note of 6 May 1942 to Al McCormack, in which Clarke wrote of the need to present the most complete Sigint information possible to the national leadership about:

> *All those associated with and against us with the end purpose of enabling an American peace delegation to confront problems of the peace table with the fullest intimate knowledge possible it is possible to secure of the purposes and attitudes, overt and covert, of those who will sit opposite them.*[13]

The irony is that in terms of the Russian target, this worked the other way around. The Venona breakthrough didn't happen until after the "peace table" (Tehran, Yalta. Potsdam, San Francisco). The Russians came to the table with ample knowledge of our purposes and attitudes — through information provided to them by traitors whose deeds ultimately were revealed in Venona.

In June 1942, the Navy decided to drop its diplomatic Sigint program entirely and turn it all over to the Army (with the understanding that the Navy would still receive the product). The Navy reasoned that it had more than enough to do handling Japanese and German naval systems while "The Army has no (Japanese) military systems of immediate importance to occupy their efforts."[14] The Army accepted the offer and pretty much had to admit that at that moment it had very little Japanese or German traffic that could be exploited (German traffic couldn't be intercepted from the Second Signal Service Battalion's field sites; the Japanese traffic would soon be available in great volume, but the cryptanalytic problem was tremendous). This was one of those times when the Army wondered about the wisdom of covering or expanding coverage on diplomatic traffic of countries other than Japan and Germany. Perhaps all resources should be thrown against enemy military systems. We have seen Carter Clarke's position on this.

E. The Beginning of the Russian Problem at Arlington Hall

In early 1943, the Signal Security Agency had two major cryptanalytic and production elements. Section B II dealt with foreign code systems, including enciphered codes. Major Solomon Kullback, a pre-war civilian employee of the agency headed that effort. Section B III, under Major Frank Rowlett handled foreign cipher systems. This somewhat odd division of effort reflected the opportunities available to the agency and would soon be changed with the major breaks into Japanese army and Japanese military attache systems.

In the B II weekly report for the week ending 6 Feb 1943, Major Kullback included this short entry: "Russian: This section activated during the past week." In his report for the week ending 13 Feb 1943, Kullback had little more to say about the Russian problem except that some of the "Material edited and sent to the machine room." With that the trail grows cold and we see no more reports from the Russian unit for six months.[15]

[12] Clarke is one of the most important figures in the history of U.S. intelligence. He, more than any other individual, deserves credit for the post—war unification of Sigint. He arranged the Army's acquisition of Arlington Hall, Vint Hill Farms and Two Rock Ranch early in the war. He founded the SSO system and played a part in the creation of AFSA, NSA and CIA. He was, said Frank Rowlett, "a very unconventional man and he was also a man of considerable moral courage."

[13] From Volume I of the Papers of Colonel Alfred McCormack, in 3 volumes, NSA Archives, CBRF 42. McCormack, a law partner of John J. McCloy, had offered his services to the War Department after Pearl Harbor. McCloy and Secretary Stimson turned him loose on G–2 to examine the handling, analysis and dissemination of Sigint. The end result was Special Branch, headed by Carter Clarke with McCormack his deputy.

[14] John R. Redman, OP–20–G, to the Vice Chief of Naval Operations, 25 June 1942, subject: Cryptanalytical and Decryption Operations on Diplomatic Traffic. Author's collection.

[15] Weekly Reports of Section B II, NSA Archives, CBTB 34.

However, we do have one other significant report from that time, from a supporting organization, and some important anecdotal information.

In a memorandum of 15 Feb 1943, to Major Kullback, Mr. Sam Snyder, head of the Arlington Hall effort against the Japanese military attache systems reported:[16]

> *This week the work of identifying and compiling the Russian codes which have been transmitted in JMA was begun. At present the most recent of these Russian Codes is being compiled — a four-digit, two-part code called '024B' which was sent to Tokyo in November and December of 1942. As the messages in which these codes are transmitted are from blind stations and are sent at very high frequency, they are quite difficult to read because of the many garbles.*

Snyder based this report to Kullback on a preliminary study that had been completed several days earlier, to "record all quickly available information concerning Russian codes which have been transmitted in the Japanese Military Attache (JMA) system of enciphered codes".[17]

This research took place in direct support of the Russian problem just begun by Lt. Zubko and Miss Grabeel. If there was any single reason for the timing of the startup of the Russian problem, it probably came from information obtained from JMA, an enciphered code system that had been in use since Feb 1940 for communications between the Japanese Army General Staff and the Japanese military attaches.[18]

In a note for file on 21 Sep 1942, titled "Remarks on the Employment of the Russian Alphabet Supplement of the Japanese Military Attache Code", Snyder commented on some messages of 21 Oct of the previous year, Helsinki to Tokyo noting that when Russian values were applied to these messages, groups of Russian letters were obtained. Snyder concluded that "what we have here is the decoding part of a two-part Russian syllabic code in process of transmission to Tokyo."[19] The Japanese, it seemed, had acquired Russian crypto-material from the Finns.

The timing of the decision to start the Russian problem at Arlington Hall may have been partly inspired by a message from the General Staff in Tokyo to the attaches in Berlin and Helsinki: circular #906, 6 Oct 1942, to Colonel Hayashi and Major Horose[20]. The message was translated at Arlington Hall on 29 Jan 1943 (the Russian problem began on 1 Feb) and re-translated on 7 Feb. The Tokyo message begins:

> **We have commenced the study of Russian diplomatic and commercial codes and obtained the following results. For our information let us know how you are getting along.**

[16] CCH Collection, folder of weekly cryptanalytic logs, JMA 1942–43, IV.I.4.9a

[17] Unsigned "Memorandum on Russian Codes in the Japanese Military Attache System", with the hand written inscription "Feb. 9, 1943, First Report". In the NSA Archives at CBNI 17, see folders 9 and 10. This memorandum must have been prepared in part by someone familiar with Russian and other Slavic languages, as there is much discussion of not only the Russian alphabet but also "the usual Slavonic transliteration—cf. H—(Serbian X; Croatian H)". Snyder possibly knew some Russian. Zubko knew Russian and Ukrainian, while Ferdinand Coudert, who replaced Zubko, knew Russian, Serbo–Croatian and Bulgarian. Another possibility is that Meredith K. Gardner, then working German Dip, wrote the memo. Gardner had privately studied Russian in 1937. He told me in 1993 that he defintely worked on JMA messages carrying Russian crypto intelligence following his assignment to the JMA unit in mid-June 1943.

[18] See "A Brief Sketch of BI–M, n.d.(but 1945), in Box 2 of the Sam Snyder Papers, CCH Collection, XI.K.2. JMA was subdivided into JAS and JAS–1, the basic JMA systems and JAT which would later be used by the attaches (actually the Sigint reps in the office of the attache) for exchange of information on the solution of foreign cipher systems. Crypt intelligence appears at one time or another in all the JMA systems.

[19] "SSS Diary", Box 2 of Snyder Papers, CCH Collection XI.K.2

[20] See folder marked "Jap Dip Dispatches", in the Venona Collection, Provisional Box 1.

The Japanese General Staff reported their findings on at least five separate Russian systems, giving short paragraphs on each and accounting for all the systems that the U.S. would later include in Venona. The Japanese had not solved any of the Russian diplomatic, but they had made some progress, providing enough clues to inspire an effort at Arlington Hall.

The most important information passed by Tokyo concerned the Russian Trade system (known as [redacted] in Venona). Tokyo reported that the indicators appeared in the first group of Trade message texts: "the first and second digits of the first group of the text gives the length of the message — the fourth and fifth digits give the additive page." Other important JMA messages available to Zubko and Grabeel, during Feb 1943, included:[21]

- Berlin to Tokyo, 15 June 1942, 87401–02. JMA Berlin reports that he had just received the five figure 023–A code, "which the German army recently captured from the Russians."[22]
- Berlin to Tokyo, #89200, 17 June 1942 (translated at Arlington Hall 16 Dec 1942). The attache in Berlin reports on two Russian military systems, the aforementioned 011–A, described as a high command system and 023–A, a general military system.
- Helsinki to Tokyo, #957, 19 Oct 1942 (translated 30 Dec 1942). The attache in Helsinki asks Tokyo to send him a "reference collection" regarding Russian military communications, "since Japan has had success in deciphering these messages." He also reports that Finland had stopped studying one of the major Russian (military?) systems because, "they did not have telegrams using identical additive."
- Berlin to Tokyo, #405, 21 Oct 1942 (translated 7 Jan 1943). Discussion of the possibility that the Russian high command was using a machine cipher.
- Helsinki to Tokyo (and to other attaches), #032, 11 Jan 1943 (translated 25 Jan 1943). The attache transmitted various Russian military code values and reported that the Finns had recovered about 1000 values. He also gave information on the Russian Arctic naval code. He concluded that, "It is reported that the British are directing the Russian codes." (the meaning of this latter item unknown, rlb).

More would be available from JMA (and its sub-system JAT) over the next two years, and we will return to the topic shortly.

Lt. Zubko and Gene Grabeel, therefore, had quite a bit of material to work: back traffic, current traffic, analytic assistance from Sam Snyder's unit, and the resulting texts from JMA messages that guided their analysis —particularly the understanding of cryptographic indicators. Zubko recognized that the diplomatic traffic could be divided into two major groups based on external address: Trade messages which bore the message address of the Ministry of Trade, and diplomatic messages with the Foreign Ministry address. Trade accounted for almost 75% of the traffic. Zubko also discovered (presumably guided by the JMA messages) information about the indicator group: .

[21] I have used the messages quoted in in the 9 Feb 1943 memorandum (no signature), and the messages in the "Jap Dip Dispatches" folder, previously cited, to reconstruct what was available to Zubko and Grabeel.

[22] In this message JMA Berlin also reported that,

> **Germany is anxious to get hold of code messages sent by the American Military Attache in Cairo and Kuibyshev (the Moscow evacuation point) to Washington in order to ascertain the condition of the British and Russian Armies. As this is most important material the Germans would like to get hold of it, if you can intercept American Attache telegrams from these two places and a number of other places as well, please let us know.**

> *He observed that the last two digits (01 to 50) operated like a page and that the third digit (1 to 7) gave the number of pages with 60 groups to a page) used in the particular message. He also noted that some relationship existed between the indicator group and the third group of the message.*[23]

However, neither the Japanese nor Zubko correctly identified the first two digits of the indicator group.

F. The Russian Problem Put on Ice[24]

The Russian problem had run for two months (and probably less than that) when it was mysteriously suspended. Unfortunately, the mystery remains.

One morning (March 1943) when Gene Grabeel reported to work, she was told — but she does not recall by whom — that the program had been dissolved, and that she should report to Major William F. Edgerton for a new assignment. She had no advance notice and never learned why this happened.[25]

According to Cecil Phillips, Major Bill Smith, a later head of the Russian problem, told him in 1944 or 1945, that the project had been shut down because Lt. Zubko had become too friendly with Major Geoffrey Stevens, the British liaison officer at Arlington Hall.[26] The U.S. did not share with the British the fact of the effort against Russian diplomatic communications, a policy which continued for another two, and close to three, years.[27]

Stevens and Zubko had probably met in later 1942 when Zubko, newly arrived at Arlington Hall, had been working the Japanese military attache problem (during his short tour at Arlington Hall, Zubko worked in both B II and B III). Stevens took particular interest in JMA, as it was also being worked by the British. Much JMA material was being exchanged between the US and UK, and one can imagine some discussion between Zubko and Stevens about the JMA messages that contained information on the cryptanalysis of Russian systems. But for some strange reason, surely by accident, the two-person Russian problem had been placed in the very office (a private office, not a bay) whose only other occupant was Geoffrey Stevens, who was not supposed to know what Zubko and Grabeel were doing! Gene Grabeel recalled how, given the security admonition from Frank Rowlett, she and Zubko spoke only in whispers, and she never had a real conversation with him. She saw Zubko once shortly after the program stopped, but Major Edgerton seemed to intervene, discouraging any conversation. She never saw him again.

Mr. Zubko gave me some information in a brief telephone conversation (made in an effort to set up an appointment). He said that he did not recall the names of anyone at Arlington Hall except Major Stevens, whom he had found to be a kindred spirit (both had trained as infantry officers). He did not enjoy the work at Arlington Hall and believed he wasn't suited for it. As for the abrupt closedown of the problem, he said that he was reassigned out of Arlington Hall in a great hurry, but he never knew why. He told me that he had been in contact with the Russians in Washington, in an official capacity, as "they were our allies." Mr. Zubko's later military

[23] 1/Lt Richard T. Hallock, "ZYT Report—6/8/44", Venona Collection , Provisional Box #1.

[24] Put on Ice—a favorite KGB tradecraft term in the Venona messages, meaning that an operation would be suspended or an agent deactivated until the operational security climate improved.

[25] Grabeel interviews.

[26] Stevens had been with the GCHQ unit in Singapore and had been evacuated after the Japanese invasion. Frank Lewis, an Arlington Hall veteran who made important contributions to the fundamental break into Russian Diplomatic, recalled Stevens as "brilliant". Meredith K. Gardner had worked JMA with both Zubko and Stevens, but he could shed no light on Zubko's departure.

[27] Frank Rowlett, Ferdinand Coudert and Oliver Kirby told me that the Russian problem was U.S. eyes only during 1943–45. SSA records include some contemporary references to this policy (discussed later in this study).

service included behind the lines activity in China. Mr. Zubko declined to be interviewed or to correspond on his service at Arlington Hall, citing the fact it was so long ago and he could not remember much about it.

During the research for this study we asked many interviewees if they recalled anything about the suspension of the Russian problem. After much effort, we found nothing, but at least we found that the mystery was long standing. In March 1946 Colonel M.A. Solomon, G–2, inquired about the origin and history of the Russian problem. The answer, from Lt Col James B. Greene of ASA suggests that the early history of the program was already clouded. Greene wrote that, "for reasons not known to personnel now at ASA, the Russian problem was first begun in late 1942, (employing two persons), was for some reason abandoned soon after, and was again started in the Spring of 1943." As we have shown, the project started in Feb 1943, not late 1942. A curious element of Greene's reply to G–2 is that it was drafted by Bill Smith, who perhaps wasn't anxious for the General Staff to know too much about this matter.[28]

In a paper written in 1965, "Recollections of Work on Russian" , Frank Rowlett commented that "the first Russian section was short-lived, for some reason which I do not remember it was disbanded."[29]

G. The Russian Program Resumed

As with the original short-lived program, we lack documentary material to account for the decision to re-open the Russian problem. But we do have the recollections of those who were there — once more Gene Grabeel, now joined by Ferdinand W. Coudert.

Captain Ferdinand Coudert, early head of the Russian program at Arlington Hall.

Coudert had been directly commissioned into the Signal Corps as a 1/Lt and was ordered to active duty on 24 Oct 1942. His background — should the material prove to be exploitable —was especially suitable for the Russian problem. A member of a famous international family law firm, Coudert Freres, he had BA and MA

[28] The Greene memorandum dated 12 March 1946, subject: History of Bourbon Problem" is in the NSA Archives, CBNI 21. Col Greene would have been correct in giving the date of 1942 if he had reference to the Russian weather material, briefly worked at Arlington Hall in 1942 and then turned over to the Navy.

[29] This paper, 6 pages with enclosures, is dated 11 Feb 1965. Located in CCH Collection, VII.83. During my interview with Mr Rowlett, he could recall nothing about the shutdown of the Russian problem.

degrees from Harvard, the latter in Slavic Studies, and a law degree from Columbia. He knew French, German, Russian, Serbo–Croatian, Bulgarian and had completed two crash courses in Japanese at Columbia.[30]

His early military assignments or misassignments included supply and motor maintenance courses at Fort Monmouth. He escaped from these in late November 1942 for duty at Arlington Hall, where he first worked as night security duty officer and courier. He briefly worked on the Japanese Army problem but failed an ad hoc oral language test by Colonel Doud (head of B Division, the Sigint production organization) and transferred to the German problem. One day in April 1943, Major Kullback, head of section B II called him aside for a conference in a vacant office. Kullback told Coudert that the agency intended to begin working Russian diplomatic, and that he would run the effort. Kullback did not tell him about Lt. Zubko's earlier effort. Kullback emphasized that the program was ultra secret and was not to be discussed within the agency. It would not be shared with the British — Coudert recalled that this seemed a touchy matter.

Gene Grabeel recalled that the program re-opened in about April 1943. A senior officer at the Hall, perhaps Major Edgerton, took her to meet Coudert and asked her to introduce him to the Russian problem. She and Coudert worked in two offices during their time together, at first in a room with two long tables separated from other work areas by filing cabinets. They resumed sorting the back traffic and the new material which was delivered about once a week. Just as when she had worked with Zubko, this remained a compartmented activity — she and Coudert whispered to each other or worked in silence. Colonel Doud and Major Kullback visited a couple times, but otherwise they worked alone for about two months.

The operation slowly built up with the arrival of the following people:

Josephine Miller, late May
Carrie Berry, mid-July
Mary Boake, mid-July
Helen Bradley, August
Gloria Forbes, September

Their backgrounds, similar to Miss Gene Grabeel's, are representative of the recruiting and hiring strategy of Arlington Hall during 1943. Miller, Berry, and Boake had been schoolteachers (Miss Boake with a recent Master's from the University of Oklahoma). Boake and Berry were recruited by a letter offer from the Signal Corps. Miss Berry recalled that the offer, at the grade of SP–5, paid $1800, plus a bonus for Saturday work, double her salary as a high school teacher in Dawson, Texas. Gloria Forbes came to Arlington Hall following graduation from the Mississippi College for Women. During her senior year she took a correspondence course in cryptanalysis. The War Department sent her the course materials, and she mailed her assignments to

[30] Interview of Mr Coudert in Key West by RL Benson, 15 Jan 1992. Mr. Coudert's father, Frederic, represented the French, British and Russian (Czarist) governments before and during the First World War, and he represented the democratic provisional government of Kerensky before the Communists seized power in Russia. The senior Coudert was a neighbor and good friend of Theodore Roosevelt. Mr. Coudert's brother, Frederic Rene Coudert (1898–1972) was a member of Congress from 1947 to 1958, representing the Silk Stocking district of Manhattan. Ironically, Congressman Coudert, while a member of the New York State Senate had co-chaired the Rapp–Coudert committee before the war, looking into Communist activities in the New York school system. The associate counsel for the Rapp–Coudert committee, Philip W. Haberman Jr., later joined (or at least was recruited for) the Special Branch of G–2, the organization that controlled the Arlington Hall product. Al McCormack of Special Branch noted that "Haberman keeps the committee files in his law office, and they are one of the most fertile sources of information on Communists and activities in and around New York — the G–2 people at Governor's Island have got acquainted with him." (see Personal Papers of Colonel Alfred McCormack, page 38, NSA Archives, CBFH41). The U.S. part of the Venona story is significantly concerned with KGB agents connected to the Communist Party in New York.

Washington. She never found out why the Army contacted her or got her name (Miss Boake had also been offered this course but had declined).[31]

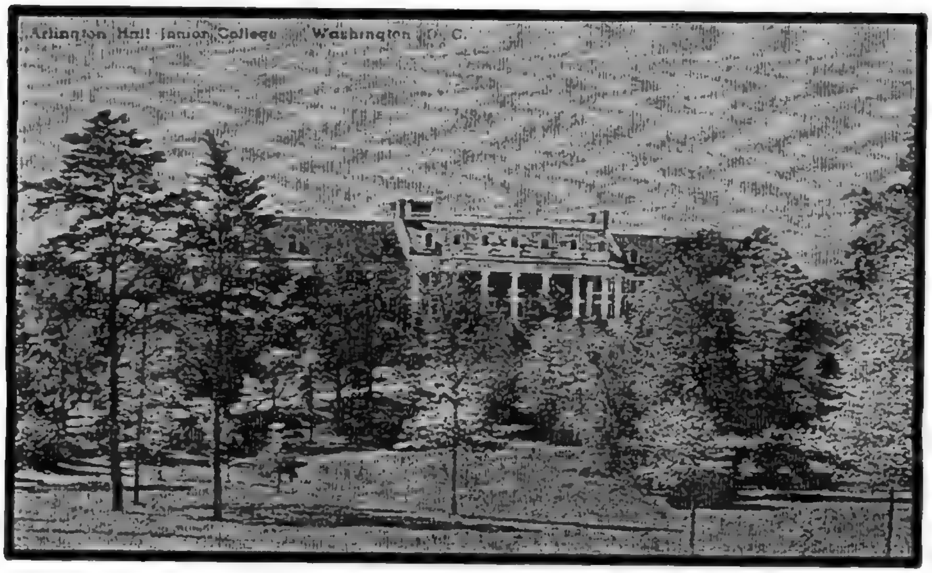
The unit then moved to a private office, for better compartmentation, but would again move to an open bay, once more defined and screened by rows of safes and cabinets.

We have no record of the earliest cryptanalytic attack on the Russian Dip systems by Coudert's unit. Russian military traffic, in low grade crypt systems, became available from Army and Navy intercept in mid-1943, and the JMA systems continued to provide information relevant to all types of Russian traffic.

G.1. More About Recruiting People for Arlington Hall

This subject seems interesting and important enough to say a little more. We have seen that Lt. Paavo Carlson recruited Miss Grabeel in Lynchburg, Virginia. Carlson's own experience is instructive in the (effective) ways of the military in an emergency.[32]

Carlson, an infantry officer, was ordered to Arlington Hall from First Army, Governor's Island. As with Lt. Zubko he didn't know anything about the place. He reported for duty on the Monday before Thanksgiving, 1942, and took care of administrative matters that day. On Tuesday he found that he had been detached from Operations (of which organization he knew nothing as yet), on Wednesday he was briefed on recruiting procedures and on Thanksgiving morning he was in Lynchburg looking for civilian recruits.



Arlington Hall before the war. This postcard was used by Army recruiters.

[31] Interview of Forbes and Boake by Benson and Phillips, 18 December 1991 in Reston, Virginia. Cecil Phillips telephoned Berry and Miller in early 1992. The Signal Security underwent tremendous growth during 1943, hiring 4067 civilian employees that year (compared to only 741 during the first year of the war), including 684 in January (the largest monthly total of the war). Space had become available with the purchase of Arlington Hall and Vint Hill Farms and the demand for people was especially driven by the breakthroughs into Japanese Army systems, notably the famous Water Transport code which was entered in early 1943. (See History of SSA, Volume One, Part II in CCH Collection, IV.B.1.1)

[32] Interview of Paavo Carlson by Benson and Phillips on 24 August 1992.

He was one of six lieutenants dispatched from Arlington Hall in late 1942 looking for college graduates to bring into the Signal Security Agency as quickly as possible.[33] Carlson remained in the field into May 1943 working out of the post office in Lynchburg and later the John Marshall Hotel in Richmond. As he knew nothing about the work of Arlington Hall, he had no difficulty with a cover story — he could only tell recruits that their employment would involve secret work near Washington, D.C. He had little contact with Arlington Hall during this period, returning there just once to file travel vouchers (which he learned about incidentally — he had assumed that he had to pay for his operation out of his own funds).

These six officers seem to have recruited the majority of the degreed people hired by Arlington Hall in 1943, and some 90% were women.[34]

H. Russian Military Traffic 1943–44

The early efforts against Russian military communications have no direct bearing on the Russian diplomatic problem. But the intercepted material did give Coudert's people some cryptanalytic experience —in fact the first decryption success against the Russian target. For Coudert himself, and Commander Taecker, his counterpart in OP–20–G, the Navy Sigint organization, it finally gave the opportunity to use the Russian language. And it inspired the first training programs on the Russian target — elementary Russian language training, Russian geography, politics and history — taught by Coudert. In any case, the chronology, if only in outline, of the beginning of the various phases of the U.S. effort against Russian targets seems important to record (the same for the UK experience).

The Army began casual intercept of Russian military traffic during 1942 (we know that weather traffic had been copied during that year and Arlington Hall briefly worked the simple crypt systems, turning the project over to the Navy in December). In January 1943, Arlington Hall published a short circular which discussed the characteristics by which Russian Army, Air Force and weather traffic could be recognized. The study included a short description of some Russian crypto procedures, call-sign procedures, net structure, and drew attention to the poor calibration of Russian field radio sets. The circular emphasized recognition of traffic rather than systematic collection.[35]

We have specific information on the beginning of the Navy's intercept of Russian military communications, as well as their cryptanalytic efforts, and of particular interest, the cooperative work of the Army and Navy.

On 6 July 1943, Lt. Cmdr. C.H. Taecker (USN ret.), a Slavic linguist and scholar, and former attache, began a study of Russian cryptographic systems, at OP–20–G, the Navy's Sigint organization. On 14 July, the Navy began regular interception of Russian traffic at Station S, Bainbridge Island, Washington using a four shift single

[33] In Lynchburg, Carlson replaced a retired Army officer, a Captain Hoffman who had been there for a short time on behalf of Arlington Hall. Hoffman, who wore a World War I campaign hat, had Carlson sit with him and a Civil Service representative for a day— then he departed.

[34] Carlson recalled that one of the lieutenant recruiters had oversold Arlington Hall in making his recruiting pitch: he showed some of the young women photographs and postcards of Arlington Hall when it had been girls school and had a riding stable and swimming pool. When these new hires arrived at the Hall they found a somewhat changed atmosphere, and the lieutenant was anxious not to come face to face with some of them.

[35] Circular, "Intercept Information, Russian Radio Operations (SIGLWO)", 26 Jan 1943. A covering letter is signed by Major Harold McD. Brown, of SSA. NSA Archives, CBTE 41. The SSA's Second Signal Service Battalion site in Alaska probably intercepted the Russian military traffic. Virtually all Russian military,naval, air, weather and police/NKVD traffic was taken from Far Eastern nets (essentially Siberia).

position watch.[36] Shortly before that, Lt Louis Tordella, OIC of Station S had received a dispatch from Captain Wenger of OP–20–G directing him to set up an isolated room staffed by his most competent operators and begin intercepting the communications of Russian naval forces in the Far East.[37] Tordella received [redacted] dated 1938 or 1939 that had been obtained from the British — probably during the Sinkov/Currier mission to Bletchley in 1941.

Tordella and his operations chief, Orville Coonce, selected the following experienced intercept operators to begin copying and studying Russian naval traffic: Harvey J. Howard, Hubert A. Price, Charles Quinn, Rodney Whitten and (fnu) Gwindon. Tordella, Coonce and the operators performed rudimentary traffic analysis. He gave this target highest priority, except when there was an emergency need for total resources on Japanese naval nets using JN–25.[38] The intercept usually went airmail to Washington, but Dr. Tordella could not recall any discussions with analysts working Russian naval back at Nebraska Avenue.[39] It was Dr. Tordella's recollection that Station S strictly took Russian naval traffic.[40]

In August the Army and Navy began to exchange traffic and Commander Taecker received three enlisted people and one civilian to work on the Russian project. This compares favorably to Lt. Coudert's resources at the time (however, Commander Taecker's unit also had a Russian typewriter!) According to an informal Navy account of those times, "it was decided by higher authorities that the Army and Navy would have joint but not combined liaison on the Russian project."[41]

By that time (and certainly by the end of the year) the Army and Navy had adopted the covername "Blue" for the Russian problem.[42] The Navy seems to have used the term "The Blue Caesar" for an ongoing series of reports on Russian radio nets and the crypt systems seen on them. Each net was named for a Roman emperor (the Nero net, the Caligula net etc.)[43] In April 1944, four additional intercept operators joined the Russian

[36] "Russian Language Section History, 1943–1948", an undated, informal survey of, despite the title, intercept, cryptanalysis and production. NSA Archives, AHA 202. Mr. Coudert and Cecil Phillips, who collaborated with Commander Taecker, provided background information about him. They especially recalled his courtly, aristocratic manners.

[37] Discussions with Dr. Tordella, 3 December 1992, Benson and Phillips. We talked about the beginning of the Russian problem and some later political and resource aspects of Venona.

[38] The Russian naval position got first place in the competition for voltage among the various target positions at Station S.

[39] Dr. Tordella thought Ham Wright might have been overseeing the Russian naval problem at OP–20–G. He did not know Commander Taecker and until our discussion had not been aware of the latter's unit.

[40] This is of interest because Cecil recalled that in 1944, both Coudert and Taecker were working NKVD military/police ciphers — however, this included the NKVD (KGB) "naval", that is coastal patrol, traffic.

[41] Ibid. Unfortunately, I find no other record of the decision or the identity of the "higher authorities". Nonetheless, the fact of the liaison is well-remembered by Mr. Coudert and Mr. Phillips, and some examples of the joint effort amply documented.

[42] Sensitive projects were color-coded e.g., the "Silver" traffic was a second in that series (and there were at least one more). However, color coding had also been used on some of the main targets, such as Orange for the overall Japanese target (Orange designated Japan in Army and Navy war plans) and later Yellow for some aspects of the German problem. Oliver Kirby described these special projects as "encapsulated programs, some of them experimental or of short duration and very sensitive."

[43] Mr Lou Maddison, GCHQ veteran and Sigint archivist, told me that the Navy's Blue Caesar program began in the summer of 1943 (discussions at GCHQ, Maddison and Benson, 6 May 1992). Our Blue Caesar papers bear no signature or agency heading, and the attribution to the U.S. Navy is based solely on Lou Maddison's information.

operation at Bainbridge and in June four operators began a watch at Station W, Winter Harbor, Maine.[44] During 1943–1944, the units headed by Lt. Coudert and Commander Taecker cooperatively worked a number of military and police systems, Lt (j.g.) Moeschl of OP–20–G working within the Russian section at Arlington Hall and Coudert and Taecker meeting weekly. Some of the Russian systems they studied included:

B–20 and B–21. Ship and air movements. Broken in 1944

B–28. Radio service messages. Simple substitution.

B–40 (ZMQ). Intercepted from July 1943. Radio service messages, postal reports in 3 digit, simple substitution.

B–43 (ZMO). Recognized in Sep 1943. Minor military administrative matters. Readable.

B–44 (ZMP/ZYP). Intercepted from Sep 1943. Minor military administrative matters and Communist Party instructions. Readable.

Much of this material was extremely simple cryptographically and rarely contained anything of interest, while other systems that might have been of interest could not be copied. Lt. Coudert recalled a Russian police or military message dealing with good places to go fishing — he said that this was a typical message. We read a comment (probably by Coudert or Taecker) about B–43/ZMO traffic, that "some of the material mentioned is rather unbelievable, and it is just possible that when an item such as 'red bilberry' [a shrub, RLB] is mentioned, it might have an entirely different meaning to the recipient of the message"; in other words, an open code underlying the plain text. Other messages concerned production of vegetable crops, care of animals and repair of railroad cars. But it was a start on Russian systems. We should mention that the Navy credits their Mrs. Leora Cunningham with "the first break into Russian cryptographic systems, by either Army or Navy" in Oct 1943, by her study of "traffic being received from both the Army and Navy".[45]

I. <u>More Japanese Military Attache Messages</u>

In August 1943, Sam Snyder, head of the Japanese Military Attache (JMA) problem at Arlington Hall, renewed his support to the Russian problem. Some of the entries in Snyder's diaries for 1943 include:[46]

- 2 August. Conference with Captain Marston re liaison with Lt. Coudert.
- 3 August. Completed compilation of messages re Russian system.
- 4 August. Spent rest of afternoon working with Mr Millard (from the Language Branch) on message re Russian Diplomatic Codes.

[44] "Russian Language Section History". Dr. Tordella recalled that in early 1945, the Skaggs Island Station, which he commanded after having been OIC at Station S, began a search for a "two channel TTY multiplex, 110–140 repitition rate" on orders from Washinton. They found the signal, developed equipment to process the traffic and reported their success to OP–20–G. He then learned that the Army SSA station at Two Rock Ranch had also begun to take Russian printer traffic (Spike Neal headed this Army program). However, in the earlier period, 1943–44, Tordella had no contact with the Army concerning intercept of Russian manual morse (which was what Station S was doing). (Benson/Phillips discussions with Dr. Tordella, 3 Dec 92)

[45] Ibid. See also these important sources: "The Blue Caesar", Report # 18 (summary up to 18 Sep 1945) in the NSA Archives, CBPI 46 and reports on each Russian military crypt system for 1943–45 in the folder "Russian Codes and Ciphers" in the NSA Archives, G030104–4. Also "The Blue Problem", a supplement to the Annual Report of B Branch, Signal Security Agency, 1 July 1943 to 30 June 1944, CCH Collection IV.c.5.6. We don't know what break Mrs. Cunningham made, but it was not in Russian diplomatic. As we'll discuss, there are several claimants at Arlington Hall for the first fundamental cryptanalytic discoveries, during 1943, about Russian diplomatic systems. The first complete decrypts of low-level Russian military messages probably date to the end of 1943 or Jan 1944. The first reading of diplomatic (Trade only) began in later 1944, but in small fragments only (such as the identification of the codegroups used to give numbers).

[46] In CCH Collection, XI.K.2. Box 2 of the Snyder Papers, Snyder diary for 2 August 1943 to 30 June 1944.

Frank Millard. He played a role in examining JMA for references to Russian cryptography.

- 6 and 9 August. More discussions with Millard.
- 11 August. Visited Lt. Coudert re Russian message.
- 13 August. Helped Millard complete messages re Russian Diplomatic Codes. Gave material to Lt. Coudert.[47]
- 19 Oct. Visited Frank Lewis who is doing a special problem for Lt. Coudert.
- 24 Nov. Major Rowlett and Captain Smith visited to see (Lt.) Mikofsky's work on Russian — arrange closer coordination both ways.

The JMA message that probably caused the excitement during August was a circular, Tokyo —> JMA Helsinki and Budapest, D 1835, sent 6 April 1943 (but not available until July or August). That message began: "We have begun to read the Russian Foreign Diplomatic Code used for communication between the Consuls in Seoul and Dairen in communication with Moscow and Vladivostok." The message contained a wealth of cryptanalytic information including the statement (after a description of the relationship of opening code groups in Russian messages) that "This gives you the starting point in the additive table, and from this as a starting point, the additives are used consecutively."

Other relevant JMA messages that Snyder would have made available to Coudert included:

- Tokyo to JMA Berlin, 29 Jan 1943 (translated 18 March 1943) refers to a 5-digit Russian code and the possibility of a Russian machine system.
- JMA Berlin to Tokyo, 6 Sep 1941 (translated 15 April 1943) in which the attache reports that "Today we received the Russian military code OCKK 7" and that the code values would be radioed to Tokyo.

The latter and other JMA messages mention the Russian crypto-material recovered at Petsamo, such as "a diplomatic code which was being burned by the Russian Consul in Petsamo was captured and reconstructed."

[47] 1/Lt J. Leslie Hotson prepared a report dated 22 August 1943, "Report on Progress of Work on Russian Codes Sent in Japanese Military Attache System", which, he noted, supplemented the 8 February 1943 Memorandum, "and should be used in connection with it." Most of Lt. Hotson's report concerns Russian military systems. On file in NSA Archives at CBNI 17.

This was KOD 26, a system used between the Foreign Ministry and the consulates and which would later be available to the US–UK for Venona purposes.

JMA, and its special crypt-intelligence subseries, JAT, continued to give clues to Russian systems for the rest of the war. Once JAT was fully solved, in about Nov 1944, a tremendous amount of material became available. It had become apparent well before then that Japanese military intelligence had Sigint liaison officers in the Axis capitols, Berlin, Budapest and Helsinki, who received and provided cryptologic materials on many allied and neutral targets including the U.S. and Russia. It had also become apparent that the Finns especially had seized important Russian diplomatic and military materials, the diplomatic at the Russian consulate in Petsamo, Finland on or about 22 June 1941 (the date Germany invaded Russia) when Germany and Finland became de facto allies. Shortly before Finland obtained an armistice with Russia in 1944, the Finnish Sigint organization and the JMA evacuated to Stockholm. But the Finns continued to cooperate with the Japanese Military Attache who also withdrew to Sweden.[48]

In a message of 18 Jan 1943 (not translated at Arlington Hall until 4 July 1945) the JMA Helsinki wired the Vice Chief of the General Staff with some concerns about the security of the JMA crypto-systems. He noted that, "Recently all countries have been devoting great energy to cryptanalysis, and they have made remarkable progress. For instance, Finland has decrypted Russian, American and Turkish codes" and "in view of these facts it seems necessary to take the utmost precautions to secure the security of our present codes." He warns Tokyo about the vulnerability of the JMA system, especially the re-use of additive key. But in conclusion he said, "I suppose that it is hazardous to instruct the higher authorities (therefore) I will cut this short."

J. Progress on Russian Dip

On 1 Sep 1943, Arlington Hall re-organized in a fundamentally important way. Section B II (Lt Col Solomon Kullback) was now to work solely on the Japanese Army target. Section B III (Major Rowlett) assumed cryptanalytic and reporting responsibility for everything else, including the Russian problem, which became known as the Special Problems Unit, designator B III b 9, Lt Coudert remaining in charge.[49]

The Russian diplomatic problem now began to receive more attention and resources. Just at about that time Arlington Hall completed a Morale Survey of each element of the agency. The report of that survey includes a short entry on Lt. Coudert's operation, giving us the names of the people then working the Russian problem and an evaluation of the operation. The people in the unit were divided into several informal units:

Lt. Coudert, OIC
Helen J. Bradley, technical advisor

Gene Grabeel
Doris Johnson
Ruby Roland

[48] The Finnish army did not cross into Russia immediately on 22 June 1941, although they had established a secret alliance with Germany by that time. A few days later the Russians pre-emptively bombed Finnish positions and the Second Russo —Finnish War began. However, the KGB and GRU and the consular people probably evacuated their Petsamo station on 22 June , but failed to destroy everything. Petsamo became Soviet territory at the end of the war. See the study, "JAT — The Solution of the Japanese Military Attache system for Crypto-Intelligence", issued by ASA 31 July 1947, NSA Archives, CBMJ 57.

[49] This reorganization was made in recognition of several major breakthroughs in 1943, especially into high grade Japanese Army systems. The tremendous volume of material, of very high intelligence value, required a maximum dedicated effort. Likewise the JMA and Purple had become a major source of information on strategic developments in Europe. JMA, all Dip and everything else that was not Japanese Army went to Rowlett.

Carrie B. Berry
Mary L. Boake
Juanita McCutcheon
Rosa Brown
Josephine E. Miller

EXEMPT

The narrative statement of work reports that the unit was receiving an average of 2500 messages per week, and the number was increasing, especially the Trade and Diplomatic. In addition to the permanent party, three clerks were loaned in to help with the logging. Further:

> *The efficiency of the unit is good. There is no idleness and few complaints or grievances arise. Thus far, the work has been negative in results. The aim is to break the systems and a staff of experts would be of value to the unit.*[50]

Indeed, the need for a "staff of experts" and a professional cryptanalytic effort was now becoming apparent, but processing the ever-increasing amount of traffic and concerns about compartmentation continued to occupy Lt. Coudert. On 3 Sep 1943 he reported to Major Rowlett that along with Russian diplomatic, including Trade, and Russian plaintext, miscellaneous traffic such as [redacted] Greek diplomatic (governments in exile) was being routed to his section, "to prevent the traffic section from learning that we were dealing with a Russian problem." The Russian traffic was being sorted according to system and lane and (external) message number; the indicators determined and handwritten on the face of each message along with the group count.[51] A week later Coudert reported that his unit had received 4000 messages during the past week, 865 Trade, 300 diplomatic, 800 plaintext "and the rest not yet characterized."[52]

The minutes of the B III Executive Council (which at various times during 1943–45 was called the Cryptanalytic Research Committee or Group, and finally the Intelligence Division Executive Council) give us some sense of the progress of the Russian problem during later 1943 as discussed by Frank Rowlett and his principal assistants:[53]

- 2 Sep. More experienced cryptanalysts needed for the Russian problem.
- 4 Sep. Lt. Coudert to give a status report with recommendations.
- 7 Sep. "It was pointed out that with regard to the Russian problem the British know nothing about it."
- 9 Sep. Both Russian military and diplomatic to be exploited as much as possible.
- 11 Sep. IBM processing of Russian traffic would be handled in a special category.
- 14 Sep. The Navy to be given duplicate copies of Russian traffic.
- 16 Sep. Major Rowlett noted Lt. Coudert's recommendations: experienced cryptanalytic people would be of value to the problem; training needed to be expanded.

[50] "SSA Morale Survey 15 July–1 August 1943". NSA Archives CBTD 31 in folder marked "Signal Security Agency". The newest employee of the unit, "Miss Johnson, recently of North Carolina" was interviewed and provided some nice personal experience information. Miss Johnson, of course, was a schoolteacher (or at least had a recent degree in education). The survey report gives a candid view of wartime civilian employment in Washington.

[51] Coudert memo for OIC, B III, 3 Sep 1943. CCH Collection, IV.c.7.4 in a folder marked "Processing of Traffic 1943". The internal serial number, that is the one-up number of the true sender (KGB, GRU etc.) was encrypted in the text, and at that stage, unrecovered.

[53] In B III b weekly report signed by Captain E.J. Wrigley. NSA Archives, CBTB 34, in folder marked "SSA Weekly Reports Jan to Oct 1943."

[53] See folder marked Intelligence Division Executive Council, 1943–1946 in CCH Collection IV.c.6.2.

- 30 Sep. Colonel Cook (head of B Branch) rejected the notion that Russian Trade material should be sent to the Bureau of Economic Warfare (note by RLB: The KGB had, as Venona would later show, significantly infiltrated the BEW).

- 13 Nov. Rowlett reported that "definite leads" had now been developed regarding the Russian traffic and that "Mr. Lewis and Lt. Elmquist should be commended for their work in this connection." However, because of the urgent demands of the Japanese problem, they would have to be relieved of from their work on the Russian program.[54]

These "definite leads" included the discovery that the Russian Trade traffic (then called ZYT by Arlington Hall) was an additive system, that is, an additively enciphered code. The Russians were using a code book of unknown size (that is, the total number of values unknown), and to each code group or value selected from the book to create the message, applying an additive to create a cipher group — the group that would be transmitted in the message. The problem then would be to "solve" the additive, and strip it off to reveal the true code group, and then obtain the individual code group values (their meaning) by book-breaking. The latter would be accomplished by tedious analysis or by somehow acquiring the right code book. The biggest problem would be to solve the additive (also called the cipher or the key). If it was from a true one-time pad it could not be solved.

Lt. Coudert's people were re-enforced during Sep–Oct 1943 by, at least, Lt. Richard T. Hallock, Mr. Burton Phillips, Lt. Karl Elmquist and Mr. Frank Lewis (Mrs. Genevieve Feinstein and Miss Mary Jo Dunning; and Cecil Phillips would come onto the problem during 1944). They were all experienced cryptanalysts —and several had strong academic backgrounds. Lt. Richard Treadwell Hallock had received a Ph. D. from the University of Chicago in 1934, in ancient Near Eastern languages. He subsequently joined the faculty of that school's Oriental Institute. During his long academic career he published many works on ancient cuneiform writing (Assyrian).

By the time these people arrived to help, Coudert's unit had been able to divide the Russian (non-military) traffic into a number of systems which he called [redacted] and [redacted] and [redacted] and [redacted] the latter two being Trade and the [redacted] systems passing as Diplomatic. Beginning in July and into December 1943, Mary Boake studied system [redacted] issuing five research reports during November and December. She reported that [redacted] (soon re-named ZZB) appeared on 24 traffic lanes but only Washington <—> Moscow carried enough traffic to work with. She concluded that none of her studies showed any particular results and the work was discontinued for some 6 months.[55] [redacted] would later be designated as [redacted] the system for Russian Naval Intelligence (GRU–Naval). Carrie Berry and Miss McClelland studied system [redacted] (later ZZC/ZZD, and still later known as [redacted]) during this same period. As with [redacted] machine runs were made with no useful results. Traffic on the Los Angeles, New York, Washington, San Francisco lanes (to and from Moscow) and the New York <—> Ottawa lanes was studied.[56] System [redacted] would later be identified as GRU.

[54] Captain Bill Smith later told Cecil Phillips that there had been some rivalry between Rowlett and Kullback on this point. Apparently some of those detailed from B II to B III to help on the Russian problem told Kullback about the breakthrough without informing Rowlett first.

[55] Informal reports on DB: 10,18,25 Nov 1943; 1 and 8 Dec 1943. Venona collection, Provisional Box #1. Mrs Hare and Mrs Hill assisted Miss Boake in these studies.

[56] Informal reports on DC: 18 Nov and 2 and 9 December 1943. Venona Collection, Provisional Box #1.

EXEMPT

On 8 Oct 1943, Coudert reported that the IBM section at Arlington Hall had completed runs on the first and last five groups of 10,000 [redacted] (Trade) messages.[57] Presumably Hallock and the others made their discoveries in this compilation, for, "The machine runs which Lt. Coudert has received have brought to light unmistakable depth for pairs of messages, and have shown some interesting relationships between groups in various positions."[58] Thus the core secret of Venona had been exposed on or about 15 Oct 1943: messages could be matched and a depth of two found, that is, somehow or other the Russians were using the same additive (key) twice. In the end, during the Venona era, this was understood to mean that the US–UK was faced with a one-time pad additive system but for which duplicate copies of some pads had been made, and the Russian code clerks were using these without realizing it. Therefore it was not, or rather some of it was not, truly one-time.

The credit for this discovery has been variously given and claimed. Lt. Hallock, Miss Berry, Frank Lewis and Lt. Karl Elmquist all have a claim. Gene Grabeel says that Frank Lewis found the first matches: she recalls the event very well and the excitement in the unit (nonetheless she noted that Lt. Hallock could have been behind it). We quote from a report that Lt. Hallock wrote in August 1944.[59]

[redacted]

Because this first break into Russian diplomatic systems is so important to the history of U.S. cryptology, it seems useful to see just how the credit should be shared. Cecil Phillips offers this account, based on his discussions with some of the participants and his review of the documentary evidence:

> *As the only real cryptanalyst on the problem, Hallock probably initiated the work of machine punching and processing the 10,000 message beginnings and endings —fortuitously, almost certainly all or the bulk of it from Washington to Moscow and Moscow to Washington Trade messages of 1942 and the first part of 1943. Had this been done a year later with the last half of 1943 and first half of 1944 traffic, the results would have been negative. Hallock may have begun his work on the Russian problem in consultation with Mrs. Feinstein, who was one of the*

[57] See Weekly Report of B–III–b–9, 8 Oct 1943. NSA Archives, CBTB 34, in a folder of B–III reports for Oct–Dec 1943.

[58] Ibid. See weekly report of BIII Research unit, 15 Oct 1943.

[59] See "ZYT Report–6/8/44" signed by Lt. Hallock. Venona Collection, Provisional box #1. Hallock is probably the author of a 15 March 1944 report on ZYT. Same folder.

EXEMPT

> *senior analysts in the technical group from which he was on loan, but she did not come to the section on a permanent basis until after the first depths were found in October 1943; or he could have consulted with Mary Jo Dunning, who was the punched card processing expert (as was Al Small).*
>
> *Frank Lewis and Lt. Elmquist came to the section to look at the hits Hallock had found and discovered that many messages before and after the seven long hits were also in depth. This would have been the real bonanza and is the kind of event that would have been reported to Kullback.*
>
> *This success probably brought Mrs. Feinstein, Mary Jo Dunning and Burton Phillips onto the problem. From there, this team went on to discover the additive nature of the first two digits, and the nature of the opening stereotype in multi-part messages. Hallock might have played a role in these latter discoveries, but I am inclined to think not, because he was busy trying to find depths greater than two.*[60]

Even before these discoveries had been made, the Russian unit had begun a major buildup of its regular workforce (Hallock and some of his associates were temporary consultants to Lt. Coudert). By mid-November 1943, the permanent party numbered 30 (eight had arrived within a week). Coudert projected a force of 79 by the end of the year and 100 by the end of January 1944.[61]

Beginning the week of 8 October 1943, Coudert had started an expanded training program for his unit. This is a milestone in the history of the Russian problem. Coudert had earlier introduced his people to the target country by teaching an area studies course on the Soviet Union. The new training program included: twelve people taking a cryptanalysis course that consisted of three half-hour lectures and six hours of study per week; six people taking a Russian language course (taught by Lt. Coudert) consisting of three hours of instruction and six hours of study per week.[62]

Building on Lt. Hallock's discovery, the unit continued to find matches in the traffic. The cooperation with the Navy proceeded. Lt. Coudert's final report as OIC of the Russian unit, 19 Nov 1943, gives a good summary of this:[63]

> *In the (Trade) system, work has been devoted mainly to finding further matches between series of initial digraphs. A considerable number have been found. Many of them were between ...... Washington–Moscow and Portland–Moscow.*
>
> *These matches give a basis for additional overlaps. Nowhere, however, do we have a depth of more than two, and evidently some other means will have to be found to achieve an adequate depth.*

[60] Cecil Phillips's sources include Captain Bill Smith — in the summer of 1944, Smith (who had replaced Lt. Coudert in late Nov 43) described these events to Cecil. Smith in turn had learned this information from Frank Rowlett as part of his in-briefing. Bill Smith's story about the difficulties between Rowlett and Kullback over the work of Lewis and Elmquist "is almost certainly true because neither one of them set foot in the Russian section for some years after." Cecil continues that, "Smith also told me that Burton Phillips proved that the first two digits of the indicator were from the second key group on the page. Hallock's account attributes the discovery of the opening stereotype in multi-part messages to Mrs. Feinstein and Mary Jo Dunning — who often worked as a three person team with Burton Phillips."

[61] See the B–III weekly reports cited above; also the file "Correspondence of the General C/A Branch 1943–1945 in the CCH Collection at IV.c.3.3.

[62] Ibid. See B–III–b–9 report for week ending 8 Oct 1943. I do not know who gave the C/A lectures. Coudert's Russian language students, the first of many thousands, later included Trudi Levenger and Bill Doherty (per recollections of Mr. Coudert and Cecil Phillips).

[63] Ibid. See B–III–b–9 report 19 Nov 1943

> *Lt. Hall and Miss Clarke of the Navy visited (us) on 16 November. They were informed of the recent developments in the (Trade) system. Lt. Hall described the work done by the Navy on radio traffic.*
>
> *A frequency list based on 10,018 words from Russian plain text messages was received from USN.*[64]

K. UK Work on the Russian Problem 1930s–1944

The Official History, British Intelligence in the Second World War, by Professor F.H. Hinsley (and others) contains this statement about UK work on the Russian problem:

> *All work on Russian codes and ciphers was stopped from 22 June 1941, the day on which Germany attacked Russia, except that, to meet the need for daily appreciations of the weather on the eastern front, the Russian meteorological cypher was read again for a period beginning in October 1942.*[65]

The matter is more complicated than that and no definitive statement seems possible.

During the 1920s and 1930s, GC&CS (now GCHQ) had worked Russian diplomatic, Comintern and military traffic. The Comintern (Communist International) traffic, exploited from 1930–1937, is known as Mask.[66] The British and Indian Army intercepted Russian military traffic from sites in the Middle East and India. We have seen that GC&CS had a body of Russian military and NKVD crypto material, obtained from the Finns by Colonel Tiltman in 1940.[67] Russian Diplomatic traffic to and from London, which included the KGB and GRU traffic, was passed on international commercial circuits and, from later 1940, on national circuits too. According to the GCHQ account:

> *Few governments allowed the establishment of a national link from an embassy. London unfortunately was an exception to this and the Soviet Embassy was not only allowed but even helped to set up its own radio links with Moscow*[68]

Therefore, the GRU, and by 1941 the KGB, had a dual system for communications, ILC and NDC. The former could be covered by [redacted] copy, the latter required intercept — at a time when the wartime demands had to be given first priority. It is difficult to tell what was collected because most of the intercept and message logs no longer exist. But it is certain that nothing could be read at that time (actually 1939–41 Venona material hasn't ever been exploitable.) We return to the murky events of 1941. Professor Hinsley suggests that all cryptanalytic work on the Russian target ended on 22 June 1941 when the Germans attacked Russia, but he does not say that collection stopped. Field Marshal Sir John Dill, the senior military representative in Washington of the Prime Minister and British Chiefs of Staff, told General Marshall in December 1942 that, "in June 1941, upon the

[64] The Navy's work on radio traffic probably refers to "The Blue Caesar" series of reports on Russian military radio nets in the Far East. Commander Taecker prepared the Russian word frequency list using Russian plaintext that the Army had given him.

[65] London, HMSO, 1979. Volume One, page 199. Professor Hinsley served at Bletchley Park during the war.

[66] [redacted]

[67] See the subsection on the Sinkov mission to the UK in 1941, above. In some notes written in 1951, Oliver Kirby, then heading the Russian problem at AFSA, wrote that, "no Comint center, allied or foreign, has read any Russian Armed Forces high level additive traffic since early 1940 when the Russians introduced the secure cryptographic systems which they continue to use" Perhaps a reference to British success before early 1940.

[68] "Soviet 'Diplomatic' Traffic on the London Link 1940–1949: A Survey" GCHQ. 3/NBF/C22, 17 Feb 1975. Venona collection, box 012, folder: S/NBF/C.

German invasion of Russia, Y Board decided to stop working Russian service traffic." (emphasis added) The Y Board made high level Sigint policy, so this represented a national decision.[69] However, the Russian section at GC&CS was not closed down until December 1941, six months after the reported date of these decisions.[70]

Sir Peter Marychurch told me that "C" (that is Sir Stewart Menzies, Chief of the Secret Service and titular head of GC&CS) gave the order to stop working the Russian problem in early 1942.[71] We also have an outline of these events from Hugh Alexander, onetime head of cryptanalytic research at GCHQ, which included the Venona program:[72]

> *A. General Order in 1941/42, implemented by Tiltman to stop work on Russian and destroy material.*
>
> *B. Cancellation of this order so far as service material went in Jan 1945 with the setting up of Pritchard's covert party at Sloane Square.*
>
> *C. Continued destruction, or non-interception of (Russian Diplomatic) until Sloane Square party returned to GCHQ in July 1945 and work on Russian became overt.*

The reference to Colonel (later Brigadier) John Tiltman concerns his statement that he ordered the destruction of Russian Diplomatic traffic. But the date(s) seem unclear—did Tiltman refer to housecleaning after 22 June 1941 to get rid of unreadable traffic of a country no longer a Sigint target? Or did he mean that collection continued and at some later time, perhaps 1945, he pitched the accumulation of the still unreadable traffic? In an interview in 1979, in which, incredibly, the most important part had been erased from the tape before transcription, Tiltman said this:

> *(Missing portion) Russian traffic to be destroyed. We had a room full of it. Not being sorted you know.*
>
> *I don't know whether I told you or not, if I mentioned the fact that years afterward when we were talking about Philby (someone) said to me in the middle of a meeting, 'If you hadn't taken that action the whole future of the world would have been changed'*
>
> *I was able to take (blame?) even though I didn't have to. We weren't sorting it, couldn't do anything so we just threw the lot away. And we regretted it afterward.*[73]

Whatever may have happened (and we speculate on this in Chapter IV), the UK was in fact working Russian targets by 1943. At a meeting that year between "C" and the Director General of the Security Service, "C" decided that some Russian systems should be worked[74] From March 1942, the Metropolitan Police and the Radio Security Service (RSS was first a part of the Security Service, MI–5, and transferred to the Secret Service, MI–6, and in either case was an intercept asset of GC&CS) discovered extensive Russian illicit radio links, apparently GRU, KGB and Comintern. "In 1943 it was decided at a high level to drop coverage (of KGB and

[69] From notes in author's collection. A copy of the Dill letter is almost certainly in the collection of G–2 Special Branch papers, CCH Collection.

7[redacted]

[71] Interview with Sir Peter Marychurch and Mr Howard Vincent by Benson at GCHQ, 5 May 1992.

[72] Message, 15 Feb 1965 from GCHQ to SUKLO Washington, Exclusive for Parker from Alexander. Venona collection, #3337, Box 13, Callahan folder #2.

[73] Tiltman interview by Dave Goodman and R.L. Benson, 30 Jan 1979, OH 01–79, CCH Collection. Cecil Phillips says that Tiltman told him, in 1946, that Russian Diplomatic had been collected but destroyed — it is Cecil's impression that Tiltman meant collection continued after 1941.

[74] Lou Maddison, GCHQ archivist. Discussions with Benson at GCHQ, 6 May 1992.

GRU) and concentrate on (Comintern), the chance of success in the Comintern field being considered much higher."[75] The Radio Security Service completely took over the intercept from the police in May/June 1943 and a covert section of GC&CS was established in London to work the material. Professor Scott headed this section and the decrypts are known as ISCOT. The first ISCOT translation, issued 21 Jan 1944, is of a 12 July 1943 message. The material was exploited through the end of the war, some in near real-time, and Scott's group issued 1484 translations. The ISCOT material, though called Comintern, looks similar to some GRU illicit and mainly concerns the fighting and intelligence gathering of Russian controlled Partisan forces in German–occupied Europe, especially Yugoslavia, Poland and Italy.[76] [redacted] It was not broken until the 1960s. The ISCOT material, of potentially great significance to UK diplomatic and military policy, seems not to have been shared with the U.S., and as we have seen, the U.S. did not share its Russian Sigint effort either.

In later 1944, GC&CS established a special section to work Russian internal non-Morse traffic (military and civil circuits).[78] Presumably this was Pritchard's covert party, working at Sloane Square in January 1945, mentioned above in Hugh Alexander's message.

The timing of all this can be considered in light of the formalization of a US–UK Sigint relationship in 1943, a relationship which has been continuously in effect for 50 years.

In April–June 1943, Colonel Al McCormack and Major Telford Taylor of G–2 Special Branch , and William F. Friedman of Arlington Hall visited GC&CS and were shown almost everything, especially the methods for exploiting and disseminating the Sigint derived from the German Enigma cipher machine. This visit followed, or coincided with, the signing of an agreement between Major General George V. Strong, Assistant Chief of Staff, G–2 and Commander Edward J. Travis, head of GC&CS, that called for a full exchange on intercept and solution data concerning Axis communications. General Strong advised General Marshall, the Army Chief of Staff, that the agreement "does not cover traffic from non-service enemy or neutral sources", an important distinction that would allow each country, in good faith, not to exchange information on Russian diplomatic, Trade or intelligence service traffic.[79]

During Aug–Sep 1943, Roger Randolph of G–2 Special Branch visited the GC&CS Diplomatic operation at Berkeley Street. He was shown almost everything, materials that could have been excluded from the agreement. In his report he puts the Russian problem under "Miscellaneous Matters" and had only this to say:

[75] [redacted]

[76] This material is of great historic interest and some of it relevant today, e.g. the traffic concerning Slovene, Serb and Croatian independence movements. Some ISCOT messages have information useful to the history of the Holocaust.

[77] I don't know how this squares with the decision to concentrate on Comintern, though that decision may have related more to processing than to intercept.

[78] Discussions with Lou Maddison at GCHQ, 6 May 1992.

[79] An original signature copy of the Strong–Travis agreement is in the CCH Collection at XI.B., Box 2 of the Carter Clarke papers. The dating of the agreement depends on how one decides who made the final decision to validate the agreement. The signature page shows 1 March 1943; the front page of the agreement is marked 17 May 1943; General Strong sent it to General Marshall on 10 June; and on 15 June 1943 Colonel Otto L. Nelson, Secretary of the General Staff approved it on behalf of the Secretary of War and the Chief of Staff. Some copies of the agreement show that Travis signed on behalf of the British Chiefs of Staff. Technically, Commander Travis was a deputy director of GC&CS (for military/naval sigint) and Commander Alistair Denniston was the other deputy director for civil Sigint (Dip, commercial). "C" had the title of Director General of GC&CS.

II. THE BEGINNING OF THE RUSSIAN PROBLEM, FEB–DEC 1943

> *Prior to 1941 Russian diplomatic traffic was studied. The conclusion was reached that it was one-time pad and accordingly the research was abandoned. At the present time Russian diplomatic traffic is not being analyzed and none of it is being read.*[80]

A final note on the comparison of the US and UK Russian programs of the time. We know that both countries closely cooperated on the Japanese military attache systems, exchanging traffic and translations of messages. In Sam Snyder's report of 15 Feb 1943, he says that packet BRZ #200, sent to London on 12 February, included a note from him to GC&CS regarding the transmission of Russian codes in JMA. His report of 12 April says that package 268 sent to London on 9 April contained "a note on Russian code messages."[81]

[80] Venona collection, box D101, in a folder marked NSA Technical Library S–7289, a series of papers on individual target desks at Berkeley Street. Note that Randolph did not say that GC&CS had stopped collecting Russian Dip traffic.

[81] See the binder labelled SSS Diary 1940–1944 (JMA), in the Snyder papers, box 2, CCH Collection at XI.K.2. Snyder surely did not mean to tell the British that Arlington Hall had started a covert Russian program. But by drawing attention to these JMA messages, Mr. Snyder could have been, accidentally, contributing to the controversy surrounding the security of the Zubko/Grabeel program.

III. The Bill Smith Era Nov 1943–46

A. Change of Command

Early leaders of the Russian program: Captain Coudert receives award from General Corderman, Captain Bill Smith on the right.

On 22 November 1943, Captain William B.S. Smith replaced Lt. Ferdinand Coudert as head of the Russian unit. Smith came to Arlington Hall as a civilian in 1942, and soon thereafter received a direct commission into the Signal Corps. Smith and Coudert had been classmates at Harvard. After graduation Smith took a position with the Columbia University Press, eventually becoming an editor of the Columbia Gazetteer and the famous one-volume encyclopedia that went through many editions (although an editor, Smith himself wrote some of the entries in the encyclopedia, especially on religion and linguistics—Smith knew French and the rare Breton dialect). Smith originally had worked on the French problem at Arlington Hall.[1]

Lt. Coudert remained as deputy chief of the unit and linguistic assistant; Lt. Hallock, who had made the fundamental discovery about the Russian Diplomatic systems, stayed on as technical assistant. Coudert, happy to be free from day to day administrative duties, turned to a wider range of translation activities, and he continued to teach Russian language and area studies to members of the unit, while founding other language training programs as well.[2]

The Russian unit now consisted of 34 people and had been re-designated B–III–E, the Special Problems subsection. This represented a fairly substantial commitment of resources and the unit grew steadily during the

[1] Smith, born in 1909, had a B.A. from Harvard and an M.A. from Columbia. He had two stints with the Columbia University Press, 1932–35 and 1940–42. In between he was an instructor at Providence College. The French problem at Arlington Hall was actually several problems, based on crypt system and target entity—Free French, Vichy and Swiss [redacted]

[2] Mr. Coudert told me that he helped the Balkan Section on Bulgarian and Serbo-Croatian material (including the translation of a letter to the U.S. from General Mihailovich, the Chetnik leader). Also, see Volume 2 of the History of SSA, p. 190–191 that states, "The Slavic languages were at first represented by Captain Ferdinand Coudert, who did much of the preliminary research", and that Captain Coudert "devised linguistic tests to determine the fitness of the personnel for this sort of work and began a training program in the minor Slavic languages."

next year, in spite of the demands for ever more people to work the Japanese Army systems and to begin a significant German military program. In an interesting think paper written at the request of Colonel Cook, head of B Division (Sigint production), R.P. Oliver made this comment:

> *The alignment of powers in the next war cannot now be predicted. A few very general considerations, which must suggest that it is imperative never to relax work on Russian and Chinese systems, are all that can be seen with any clarity by the contemporary eye.*[3]

B. Developments During 1944

Captain Smith immediately began reorganizing the cryptanalytic efforts, with particular attention to the Russian Diplomatic problem. He set up procedures for message logging which, with minor changes, would continue throughout the Venona period. He established the principles of "masterblocking"—a procedure in which messages are recorded in order of original encipherment with an arbitrary master block or pad number assigned. Smith discovered that if messages were ordered first by file date and time, masterblocking would be straightforward, but messages into Moscow had to be ordered by external serial number.[4]

Smith stopped the effort against some of the Russian Diplomatic systems in favor of concentrating on the Trade systems where Lt. Hallock had found the depths. Miss Berry ceased her work on [redacted] (later found to be GRU), Miss Boake ended her study of [redacted] (later found to be GRU–Naval) and the Navy may have been invited to look into the other Dip system (later found to be the true Dip Consular system [redacted]. We have no contemporary record that much had been done on the [redacted] systems, later identified as KGB and which would be the heart of Venona. Work on all these systems shut down until July 1944, with all attention given to the Trade messages. Cryptanalytically this made good sense. It represented by far the greatest volume of Russian Dip and a small but vital beginning had already been made in breaking it—the discovery of depths, that the same key appeared at least twice for a large number of messages.

Still, in retrospect, some of the objectives or methods seem unclear. What would be called the [redacted] systems, that is the messages of the Soviet Purchasing Commission to and from the Ministry of Trade in Moscow, had been identified right away, by Lt. Zubko as just that. The intelligence value of these messages, even if read in real time (and none could be read at all during the first year of the Russian problem), could not have been expected to be high. Certainly the messages on the U.S.–Moscow lanes would have been expected to contain information we already knew: endless lists of parts, equipment, goods; shipping data; terms and dates. We were openly supplying the Russians and working out with them all the details of delivery and shipment. Yet, in a report of 30 June 1944 on the Blue Problem (Blue having become the codeword for the Russian problem) we read that the major cryptanalytic successes are to be found in the study of ZYT (at that time the term for [redacted] that is Trade), a diplomatic system, "presumably carrying intelligence of a high grade and used by many stations."[5] Probably the only conclusion we can make is that everyone involved saw this as a

[3] Paper, no heading or signature, with handwritten covering note, 4 Dec 1943. Oliver's paper is quite interesting as it concerns continuing oversight and collection of unworked systems during a time of transition.
[4] From the Hallock reports and Cecil Phillips
[5] Supplement to the Annual Report of B Branch, 1 July 1943 to 30 June 1944 : The Blue Problem. CCH Collection, IV.c.5.6.

pure cryptanalytic problem, which it would remain until Dip systems became readable—then the consumers would decide what had intelligence value and the problem would go from there.[6]

Following Hallock's discovery about re-use of key, the unit found several thousand pages of re-use, but no usage more than a second time, that is, a depth of two only could be found. This was discouraging to the cryptanalysts at that time because the conventional wisdom was that re-uses had to be greater than two to be solvable. [redacted] This attack, completed in March 1944, failed to produce any results. Hallock also considered a possible attack in which tentative key groups from the existing re-uses might be tested against other messages. There is no evidence that he tried this at the time, but in later work all solved key was tested against all messages.[7]

Meanwhile effort continued to fully explain the message indicator of the messages where re-use had been found and to recover some code groups from the re-uses already found. About half of the case of re-use did not have the same key page number, but in all cases the first two digits of the indicator were identical if the messages were in depth from the beginning. The Japanese had suggested that these two digits were some form of row and column coordinates, but Hallock's group had also discovered that when these digits were subtracted from the first two digits of the third group, the resulting dinome was not randomly distributed. According to Captain Smith (in a discussion with Cecil Phillips in 1944) Burton Phillips concluded that the two digits in the indicator were key and that the non random result was two digits of code. While we have no information as to how he arrived at this conclusion, it was clearly proven by the next major success on the depths—the discovery of self-checking code groups for numbers at the start of many messages. Miss Berry recalled that she either noticed or identified some aspect of the Trade indicator in later 1943. Since Miss Berry was working closely with Burton Phillips at the time, her discovery may have related to the two digits of key in the indicator which Burton Phillips apparently confirmed.[8]

It had been observed earlier that the code digraph among the long messages which appeared to be parts were different from shorter messages. These messages were almost uniformly about four pages or 240 groups in length, and the non-random digits derived by subtracting the first two digits of the indicator from the third usually began with a zero in the second and succeeding members. Further, it had been observed that the digraph was 01 for a long sequence and later became 02. According to Hallock's reports, this led Mrs. Feinstein to suggest that this might be representation of some continuation message number of the previous message. This proved to be true—and even better—it turned out to be a representation of the external number of the preceding message—providing an almost certain four group crib into the first four groups of the message. At about the

[6] Throughout the research for this study we asked veterans of the problem if they had ever been briefed on what to expect in the traffic, particularly if they had been directed to look for probable KGB or GRU systems. No one recalled ever having been told what to look for—from a content standpoint—and no one ever had a briefing from G-2 or the FBI for example about the Russian intelligence services. It was seen as a cryptanalytic problem—the nature of the traffic would be revealed by breaking into it and reading it.

[7] Cecil Phillips provided, and largely wrote up, all the technical information in this paragraph and others in this section. He is a primary source for the history of Venona.

[8] Cecil Phillips; also Cecil's discussions in 1992 with Carrie Berry.

same time the code groups for numbers were found to be numeric code groups of a clear self-checking variety—which enabled virtually instantaneous determination of the form of the 1000 code groups used to express numbers.[9]

The Russian unit moved in January 1944, into a larger work area, but one typical of most of the work areas of Arlington Hall. They occupied an open area measuring about 50 x 50 in the back of the second floor of the B Building. Their space was separated from the rest of the open wing, occupied by the weather section, by large wooden screens that were some seven feet high and four to six feet wide. A small opening between the screens provided the entrance to the "office". Captain Smith sat at a long table to the left of this tiny entrance, with his back to the partitions, seated so that he could watch everyone at work and coming and going (as they had to squeeze by him). This was truly another era— the section had only a couple of desks, otherwise everyone sat two-by-two at tables seated on old, cast-off and unmatched chairs. The unit had just two or three standard typewriters and one Russian typewriter. Everything except paper and pencils was in short supply. The place was not airconditioned. The unit, officers and civilians, worked a six day week (but were not paid a full day's pay for Saturdays).

Security was especially tight in the Russian section. Those studying Russian under Lt. Coudert had to lock up their language books and dictionaries; maps of Russia came off the walls at the end of the day. Smith and Coudert admonished everyone to talk in a low voice and to avoid discussing their work with anyone else at Arlington Hall. At the end of the day all the cabinets were locked and the classified or target-revealing trash put in a special container.[10]

Unfortunately the KGB seems to have already heard about the Russian problem at Arlington Hall and their stooges were hard at work trying to learn the details.

C. Lauchlin Currie, the Silvermaster Ring and the KGB: Spring 1944

In November 1945, Elizabeth Bentley, a veteran KGB agent, gave the FBI a 107 page statement (See section I. of this chapter). Among the many startling revelations about KGB espionage in the the U.S. was this:

> *During this same period I became aware of the fact that Lauchlin Currie was friendly with the SILVERMASTERS and was particularly friendly with GEORGE SILVERMAN. To the best of my recollection, Currie did not supply SILVERMAN or the SILVERMASTERS with any documents, but used to inform SILVERMAN orally on certain various matters. As an example of the information orally furnished SILVERMAN, I recall one occasion when CURRIE informed him that the United States was on the verge of breaking the Soviet code.*[11]

Unfortunately, Miss Bentley did not give a date for this incident, nor can a date be determined by the phrase "During this same period". However, as later investigation would show, it was most likely March or April 1944.

Currie, born in Nova Scotia, was a prominent academic economist connected to the Roosevelt administration from 1934–45. He received a PhD from Harvard in 1931, became a U.S. citizen in 1934 and taught at Harvard and the Fletcher School of Law and Diplomacy. In 1934 Treasury Secretary Morgenthau

[9] Cecil Phillips. Cecil believes that at this time, while Burton Phillips, Genevieve Feinstein, Mary Jo Dunning and Captain Smith were making these discoveries, Gene Grabeel was supervising the rest of the unit, carrying out the most basic cryptanalytic tasks upon which the success of the others was built.

[10] As recalled by Cecil Phillips, Gene Grabeel, Ferdinand Coudert; also see the report on The Blue Problem, previously cited. Miss Grabeel recalled that Lt. Coudert was especially concerned with security and talked to people often about it—we should also note that Coudert made a lasting impression, entirely favorable, on those who worked for and with him.

[11] Statement signed 30 November 1945, NY Field Office, FBI. A copy of this statement is in the Venona collection.

appointed him as a senior analyst for the Treasury Department; in 1939 he became an administrative assistant and economic advisor to President Roosevelt. He held that position from 1939–41 and intermittently thereafter, and during the war years had at least one stint as temporary stand-in for Harry Hopkins. He performed various special missions during the war including a fact finding mission to China.

In 1947 Currie denied to the FBI that he had told Silverman that the U.S. was on the verge of breaking the Soviet code. Currie did say that he might have heard about such codebreaking developments in view of his contacts and position. He said that he would have had no problem telling Silverman that type of information but did not recall having done so (Silverman, an employee of the Air Staff at the Pentagon had a clearance, though no known official access to Sigint— and obviously no need to know regarding the Russian problem). In a December 1952 appearance before a Federal Grand Jury in connection with another matter (not involving himself), Currie was asked about the codebreaking matter. He denied ever discussing this with anyone. When reminded of his previous statements to the FBI about Silverman, he said that he would not have told Silverman such information (but he didn't say that he knew that information anyway).

In her 1951 book Out of Bondage, Miss Bentley did not mention the codebreaking incident. However, she made a brief reference to it in her six part series in the New York Daily Mirror. Upon reinterview by the FBI, Miss Bentley dated the incident to the Spring of 1944. She recalled the considerable rushing about by Currie, Silverman and Silvermaster to get this information to the Russians and then to follow up. At that time Silvermaster controlled a major KGB net; Bentley was an auxiliary agent handler and the courier between Silvermaster and the KGB. Bentley said that she verbally reported to her KGB superior, "Bill", the information that some agency of the U.S. government was on the verge of breaking the Soviet code and "they almost had it". Bill then said to her, "Well is it a trap or isn't it a trap?" He told her that her network had the "assignment and duty" to determine the particular code the Americans were about to break. Miss Bentley said that while she and the Silvermaster net worked on this for a time, they never learned which code was about to be broken (nor did they learn anything else about the U.S. Russian Sigint program—at least Miss Bentley could give the FBI no further information on this matter.).[12]

Venona would prove that Miss Bentley's statements about KGB activities in the U.S. were extremely accurate. Nonetheless, her Currie story might be considered a bit slim on detail, and it has not been found in Venona. However, the FBI found two independent witnesses. One, a senior government official (name withheld) who worked closely with Currie during the war, said that Currie told him that he (Currie) had revealed to the Russians that the U.S. had "broken the Soviet Diplomatic code". Currie was disturbed that the U.S. had done such a thing, and because he believed it wrong, he said that he had "tipped off" the Russians.

In later discussions with the FBI this official recalled his conversation with Currie in greater detail, placing it in the Spring of 1944 (though he said it could possibly have been as late as Fall 1944). The official reported that Currie raised this matter by telling him that he knew of a very hush-hush matter, too sensitive to talk about. Currie then proceeded to tell him that he had learned that the U.S. had broken the Soviet Diplomatic code and that this was a terrible thing to do to any ally "and indicated our lack of trust in the Russians." Currie said that he had fixed this by telling the Russians, while assuring them that he, Currie, did not approve of such activities. Currie said that by his actions he had prevented the sowing of seeds of distrust between allies. Currie did not tell this official how he had learned about this and gave no details about the code that might be involved. The official rebuked Currie. The official said that he had later described this incident to Frank Wisner of CIA and to members and staffers of the House Committee on Un-American Activities including Robert Stripling, Ben Mandel and Richard Nixon.

A second person associated with Currie during that time recalled that Currie said that the U.S. had broken the Soviet code. But that source said that her recollections were too vague for her to be good witness in any proceedings.

The FBI contacted NSA for assistance in this matter. General Ralph J. Canine, Director, NSA told the Bureau on 9 Dec 1953 that to his knowledge no Russian codes had been broken in 1942 or 1943. In a memo of 25 January 1954 General Canine told the FBI that the Army and Navy made no decryptions of Russian systems until 1945. On 12 Feb 1954, the Washington Field Office advised Bureau headquarters that:

> *It has been determined by NSA that in 1943 work on Soviet codes was initiated by both the Army and the Navy and that in early 1944 limited success was had with one Soviet system not strictly a diplomatic code. It was also ascertained that decrypts of messages were shown to President Roosevelt by a United States Naval Officer whose duty it was to take the decrypts to the White House and that Currie could have learned of the contents of some of them in that manner. For your information, NSA is making efforts to identify the Naval Officer whose duty it was to take the decrypts to the White House.*

NSA was not able to make this identification.

The Agency could have done better, in the Currie case and in the Weisband case, as we will discuss in a later part of this study. Suffice it to say that the FBI interviewed a lot of officers who had been in liaison with the White House, including Colonel Frank McCarthy, former Secretary of the Army General Staff and (later producer of the movie "Patton") but found very little. One officer, however, reported that daily summaries of Russian decrypts had not been prepared , "for this code had not been broken sufficiently ".[13]

Did the KGB react to Lauchlin Currie's information?

D. <u>May Day 1944</u>

On 1 May 1944, the KGB changed the indicator system for its encrypted international communications, that is for the enciphered code used by the Residencies and the Moscow Center. This change had been made on short notice although that would not be known until the Venona breakthrough, at which time the following message, from Moscow "To all Residents", dated 25 April 1944, was decrypted and translated:

EXEMPT

[13] Ibid. My point is this: In the early 1950s, many people at NSA could have told the Bureau exactly what was going on in the Russian program during 1943–1944. Carter Clarke [redacted] could have helped. The lead suggested by NSA—to search for a naval officer who gave Sigint to the President—was preposterous and cannot be seen as anything other than misleading. I have not been able to find NSA records on any of this. AFSA had been similarly unhelpful to the Bureau in the Weisband espionage case—see Chapter VII.

> **From 1 May, instead of the method of setting up the indicator group in effect at the present time, for the determination of the reciphering table enter in clear the beginning of the cipher text the first group of the table with which the leaf of the pad (on the occasion?) begins. The recipherment itself begins with the second group of the table. At the end of the cipher text enter, likewise in the clear, the group following upon the last used group of the (additive key) (the second indicator group). If the recipherment ends with the last group of a table, enter the first group of the following table, ----------[note by RLB: thereafter some 89 groups of the message could not be exploited][14]**

Cecil Phillips has observed that this indicator change was the KGB cryptographers second most important contribution to the cryptanalysts at Arlington Hall (first place going to the original flaw: the manufacture of extra sets of 'one time' key pads). The change had to do with the 'indicator' that showed what key page, from the pad book, was being used by the message sender. The timing is such that it suggests some connection to Currie and Bentley getting the word to the KGB that the Russian Diplomatic code was about to be broken. As a security measure it doesn't make much sense, but as the change was introduced in such a hurry, it does arouse suspicion. In any case, the KGB cryptographic directorate could have made the change merely to be able to tell Beria (who presumably would not have known the difference) that something was being done in the face of the information that the KGB New York might have told the Center when they got the report from Bentley (thru many KGB intermediaries in Washington and New York). That something does not make sense cannot be taken as proof or disproof.

Quite possibly, the indicator change was made for reasons other than the incomplete, and at that time inaccurate, information from Currie.

The indicator change on May Day meant the replacement of a fairly simple 2 digit key page indicator which had been in use for at least four years with a free 5-digit additive group from the key pages at the start and end of each message. The earlier system, the one replaced, and which during the Venona period would be called [redacted] by US–UK, provided a key page number in the last or next to last group—derived by subtracting a pair of digits representing units and tens digits of group count (which occurred as the first two digits of the indicator) from the third and fourth digits of the indicator group.[15]

The new indicator system resisted solution for about six months. During this period, Miss Berry and others tried all the conventional means of indicator solution—mostly subtracting one message group from another, which had been the basis for a number of indicator systems up to that time. None of these attacks produced any results.

EXEMPT

[14] This message, a circular, was sent by the Center to the KGB stations in Havana, New York, Mexico City, Ottawa, San Francisco; the same message must have gone to the other Residents too (e.g. London) but in a message(s) that has not been broken. The message was translated by Meredith Gardner at AFSA by 1950, but not translated and reissued in later years (as most of Mr. Gardner's early translations were).

[15] Cecil Phillips provided all the technical data in this section. During the course of the research, which was a joint project, Cecil wrote many short essays—on individual topics and for general overview. Here I cite, and almost copy verbatim, from his essays "May Day 1944" an[redacted]–The Beginning". These are held in the Venona Collection with other research files.

III. THE BILL SMITH ERA NOV. 1943–1946

In late September or early October 1944, Cecil Phillips and Lucille Campbell, who had been recovering key on a Far Eastern NKVD troop system, undertook on a parttime basis the solution of the new system. Phillips, a 19 year old cryptanalyst, had been at Arlington Hall for a year, joining the organization after his sophomore year at the University of North Carolina.[16] He had joined the Russian problem on May Day 1944.

[redacted]

Cecil Phillips (top left) and Frank Lewis (lower left). They made fundamental breaks into the KGB system in 1944. Venona veterans Bill Lutwiniak (top center) and Paul Derthick (top right).

During much of the period described above, Lt. Hallock had been studying the biased key distributions found in depths, searching for clues as to how the key might have been produced. As the section's senior cryptanalyst, Genevieve Feinstein had been following Hallock's work and was well acquainted with his findings of key families. In mid-November 1944, Mrs. Feinstein, upon reviewing the studies of distribution made by Phillips-Campbell, observed that this looked like "free" key and ought to be tested against the Hypothetical,

[16] Cecil Phillips had been a chemistry major at UNC. As he had been classified 4–F by Selective Service, his mother suggested that he go to summer school or get a job. He went to the U.S. Employment Service in Asheville to inquire if the government could use a chemistry student. The USES directed him to a Signal Corps lieutenant who was at the Post Office recruiting for Arlington Hall. The officer gave him a short written IQ type test. Within two weeks he was at Arlington Hall. He worked the Japanese weather problem most of his first year and transferred to the Russian problem on May Day 1944, the day the indicator change took place.

Additive Bank that the unit had recently produced by predicting the opening code in Trade messages, and then card punching the results to produce an index.

Genevieve Grotjan Feinstein, principal cryptanalyst in the 1944 break into the KGB cipher system.

"Free" key meant that the message text included as a first cipher group key taken from the opening group at the top of the pad page, in other words the cryptanalyst was "seeing" the opening group from a KGB one-time pad sheet. By knowing the true value of that opening group it would be possible to quickly look for matches by taking that true value and looking for the same value in another message (which might or might not be in the KGB system—more likely it would be in a Trade message). If that same value was found, in the right place in the message, then the cryptanalyst knew that the same pad page had been used twice. A match in a depth of two—enough for Arlington Hall to eventually break into the matched messages.

At the direction of Burton Phillips, Katurah McDonald and two clerks who worked for her began testing Mrs. Feinstein's hypothesis. The results were quick and dramatic, for the testing began to produce repeated opening code phrases in New York to Moscow KGB messages. Thus, the May Day indicator and the first reuse in [redacted] (the name that would be given to KGB systems) were found simultaneously. In a few days—and this is still in November 1944— several hundred pages of key reuse were found and the work on some of best parts of Venona began. But the nature of the [redacted] text was not apparent for two more years. Nonetheless this was the most important single cryptanalytic break in the whole history of Venona, and, like the fundamental discovery of reuse of key, has merited the naming of names.[17]

EXEMPT

[17] In some of Meredith Gardner's notes, this breakthrough has been dated to Feb 1945 [redacted] GCHQ historian of Venona and a veteran of the program, used Mr. Gardner's date). We move it back to November 1944 based on Cecil Phillips' recollections and papers he reviewed about the attack on [redacted] the Russian consular system (and one of the Venona systems).

E. Carter Clarke Delivers a Warning to Arlington Hall

General Carter W. Clarke.

We have discussed the activities of Lauchlin Currie and have outlined the story of the May Day cryptographic change. These could be related, but we cannot know. The third part of this story seems even less clear, but it needs to be recorded; and then we can try to summarize and offer some explanations for these events of 1944.

According to Frank Rowlett, who in 1944 headed the General Cryptanalytic Branch at Arlington Hall (which as discussed earlier meant all Sigint targets other than Japanese Army), Colonel Carter W. Clarke, head of G–2 Special Branch and controller of Army Sigint policy, visited him and Colonel Harold G. "Dink" Hayes, fairly soon after Hayes arrived at Arlington Hall, bringing an important warning from the War Department. We cannot put a date on this, except that it almost certainly took place in 1944. While Hayes had arrived at Arlington Hall in March, after heading Army cryptologic activities in North Africa and Italy, Mr. Rowlett could not really date the visit except to say that he "assumed" it was soon after Hayes "took command". Hayes took over the B Branch, the Sigint production organization, in which Rowlett was a principal subordinate at the beginning of April 1944, so perhaps the meeting was in April or May.

Clarke began by asking, "Tell me what you are doing on Russian?". Rowlett explained the Russian program. Clarke then turned to Hayes and said, "You haven't told me that you are doing anything on Russian, have you Dink?" To which Hayes replied, "No sir, I haven't" Clarke then said to Hayes, "You stop doing what you told me you were doing on Russian and Rowlett you keep on doing what you told me your outfit is doing on Russian." Clarke then explained that he was acting as a messenger for the War Department bringing an instruction from the White House, actually from Mrs. Roosevelt, that Arlington Hall was to stop working on Russian Diplomatic. Clarke described it as a cease and desist order, and they were to ignore that order. Clarke said no more, then or later, and the Russian program continued.[18]

We can only guess what lay behind Clarke's visit or exactly how the order reached him. Most likely he got the word from General George V. Strong, the G–2, acting on orders from either Secretary Stimson or Assistant Secretary John J. McCloy, probably the latter, as McCloy had oversight of Army intelligence programs and had a particular interest in Sigint. Lauchlin Currie had ready access to the White House, as an administrative assistant to the President and because of various special assignments. He sometimes sat in for Harry Hopkins, who had a number of illnesses during those years. Whether he "got to" or otherwise influenced the President or Mrs. Roosevelt on this matter is unknown; he could just as well have issued some verbal instructions to the War Department in the name of the President.

Instead of speculating along these lines, we conclude the Currie-May Day story with some suggestions about what Currie could have known about the Russian program:

- During 1944, the U.S. could not exploit the Russian Diplomatic code; no one in the know could have suggested that we were on the verge of a breakthrough until, at the earliest, later November 1944. Even then such a prediction would have been unlikely.
- However, the White House may have been informed by the War Department or Navy that the U.S. was working Russian systems and could have received some not very interesting translations from Russian military/police systems — but nothing from Diplomatic. Currie could have known about all this.
- Just as likely, Currie could have taken what he heard about the U.S. effort against Russian communications and leaped to some conclusions, given his almost certain knowledge of the extraordinary US–UK successes against Japanese and German communications.

In a later part in this study we will review some Venona decrypts relating to KGB access to the White House and the possible identification of Currie in the traffic.

[redacted]

[18] Rowlett interview by Benson, 14 Jan 1992, Sarasota, Florida; Rowlett interview by Hank Schorreck and others, 31 August 1976 and after, at NSA, CCH Collection, transcript of Rowlett interview.

EXEMPT

[redacted]

EXEMPT

EXEMPT

[redacted]

G. Slow But Steady Progress at Arlington Hall and Nebraska Avenue 1944–1945

By the end of 1944, Captain Bill Smith's Russian unit at Arlington Hall had 18 cabinets full of diplomatic traffic, none of which had been read, representing about 150,000 messages in all the Russian Dip systems (including Trade) of which only 10% had been found to involve reuse of key, meaning that only the latter could potentially be solved. In the next 5 years, another 700,000 or so Russian Dip/Trade messages were collected, and about 15,000 of these also involved reuse.[25]

During 1944, the unit mostly worked Trade messages, which represented the bulk of the traffic, though as we have seen the major break in November was into what would later be recognized as KGB. That break had been made because the KGB changed its own indicator system on 1 May 1944. The KGB, though responsible for all cryptographic doctrine and production of all crypto systems, had not effected an indicator change in the other systems. From about July 1944, the systems that Smith had dropped 6 months before again came under active review. These included [redacted] and [redacted] the system identifiers later used for Consular, GRU–Naval, and GRU systems. The Navy continued its small but active inquiry into Russian Diplomatic systems, but always in consultation with the Army.

Captain Smith may have asked Commander Taecker to take over the study of [redacted] and [redacted] for some of the informal records of the time mention that the Navy had assigned a couple people to these systems. In late September 1944, Commander Taecker gave Smith a short technical report on [redacted] "drawn up by our people here (at Nebraska Avenue)".[26] Lt. Robert Carl was the Navy's principal analyst for [redacted]

The Navy's overall Russian program grew considerably during 1944. By June a 26 person unit at Nebraska Avenue was working the traffic and three small watches at field sites were intercepting naval, military and police traffic. In September, Ensign W.W. Moeschel was integrated into Arlington Hall to work military systems. During October–November, 20 officers reported to the Russian section after completing language training at the Navy's school at Boulder, Colorado. In November the Navy began publishing intelligence summaries of

[25] From Cecil Phillips paper [redacted] –The Beginning

[26] Informal Memorandum for Captain William S. Smith, Signal Corps, 28 Sep 1944, signed by Cmdr C.H. Taecker. Venona Collection, Provisional Box #1, ZZH Folder #2.

EXEMPT

Russian decrypts four times per week.[27] In December, Commander Taecker left the unit, replaced by Lt. Commander G.L. Todd, like Taecker, a retired officer recalled to duty. Some internal organizational changes were made at this time to increase security and disguise the existence of the Russian program.[28]

In spite of the dramatic success at Arlington Hall in November 1944, only modest gains were made in 1945 against the Russian diplomatic systems. Nonetheless the work during that year laid the foundation for the Venona breakthrough of late 1946. Most of the effort went into getting [redacted] (KGB) code recovery and [redacted] (Trade) code recovery to a state where context could be obtained from the matches to obtain meaningful text. We must continually emphasize that the Arlington Hall Russian unit still had no clue to the real identity of [redacted] —at the time it was seen as a modest sized, in terms of traffic volume, world wide Russian Dip system that looked susceptible to full solution. No one knew what that solution would mean in terms of intelligence.

As an example of the difficulty of the work, as of 15 April 1945, it was not yet certain that the Green trade code was a two part code, this almost 18 months since Lt. Hallock and his team had found the first reuse in [redacted] As a further example of the slowness of the effort, by February 1946 only 35 [redacted] code groups had been identified, and a year later, though 2600 [redacted] code groups had been identified, only 320 had been given Russian meanings.[29] In other words, four years after the Russian program had begun, only 3.5 percent of the values in that KGB codebook could be read. At this point it seems useful to leap ahead to give some idea of what the Russian Dip systems looked like, with the understanding that Arlington Hall, at this point in our narrative, did not know any, or much, of this.

All the Russian systems passing as Dip used an enciphered code. For the KGB (the [redacted] systems) this meant a codebook of 9999 groups, 0001 thru 9999. System [redacted] used a book of that size, with the groups being enciphered by additive drawn from the one time code pads. We have seen how the Russians changed the indicator system, which meant the system for determining which page of the one time pad book was being used. The codebook also allowed the code clerk to spell out words that were not in the codebook, a vulnerability of the system.[30] This was a centralized cryptographic program—a department of the KGB drawing up different codebooks for the different organizations involved in the worldwide Dip communications nets.

That KGB cryptographic unit also prepared the one time code pads from which the additive was taken and added to the codegroups being transmitted. Obviously, the real security was in the onetime pad additive. The KGB professionals, if not their leader Beria, much less Stalin, surely did not believe that the codebooks themselves could always be protected given the fortunes of war. Nonetheless, it was KGB doctrine to very carefully protect those codebooks. Such a system could only be broken if the opposition cryptanalyst had the one time pads or knew how the pads were generated, and thus could replicate them. The generation scheme was never determined or replicated. The only hope lay in finding reuse of pad pages. This happened through successful matching, also called finding of depths or overlaps. All these terms can be used interchangeably. While we will discuss all this later, the reuse of pads was not what one would expect—carelessness by the code clerks. Instead, the break was possible because of what came to be called manufacturer's re-use, which meant that sometime after the German invasion of Russian (22 June 1941), the KGB's pad generating center

[27] Most of the decrypts were of naval and NKVD naval ("Coast Guard") traffic. No Dip had been solved by Army or Navy.
[28] OP–20–G Russian Language History
[29] Cecil Phillips' paper, RUD—The Beginning.
[30] But a vulnerability only if the security of the one time pad was breached. The spell table was a code within a code, but it existed to give the communicant a way to spell out words and thus get beyond the limitations of the vocabulary of the basic codebook. The spell table was not as such a COMSEC system.

manufactured extra sets of pads, probably because of the pressures of the rapid German advance and the emergency conditions. However, the re-use meant that one extra set of key pad was produced but only one extra set, thus creating a depth of two but no more. In other words, one time pad A should have been manufactured in two copies only, one for the user in the field and one for that user's headquarters element in Moscow. What happened was that a second set of pad A would be manufactured and issued to different communicants. In this example, Pad A might have been issued to KGB New York and the Center; the second set of Pad A might have been issued to the Soviet Government Purchasing Commission in Washington and the Ministry of Trade in Moscow. It was a matter of finding the match. No aspect of the Venona process would be more important than working the voluminous Trade traffic to look for depths with other more interesting (from the intelligence standpoint) systems and then to recover codebook vocabulary or values.

Work on the one part Red [redacted] (Trade) code was progressing fairly well by April 1945 (one part meant that the codebook was in strict alpha-numeric order, a big help for the bookbreaker). But almost all the work was concentrated on the first four groups of each pad page, a technique that took advantage of the vulnerable stereotyping in this class of traffic. During that April, Dr. Samuel P. Chew transferred into the Russian unit, after two years on the Japanese Army problem. Chew, who had been a Professor of English at the Citadel, the University of Wisconsin, and Oklahoma had joined Arlington Hall on 4 February 1943.[31] Dr. Chew was a tenacious cryptanalyst who attacked the Trade-Trade depths with enthusiasm and undoubtedly reinvigorated the Russian unit's Dip effort. In making this attack Chew discovered a form of stereotyping in Red Code Trade messages which made solution of any of these depths much more possible. The discovery that there was a pattern—later called the "item cycle"—in which commodities and shipment amounts were listed in an order and with sum checks made some text prediction reasonably practical. This added enormously to depth reading capability of Red code against Red code and Red code against Green code (also Trade o[redacted]—and against [redacted](KGB) as well. In fact this discovery was a very major, some would say the most important, contribution to the Venona break.[32]

Fortuitously, the New York KGB messages would be matched primarily against the Washington to Moscow Trade messages—the messages with the most stereotyping ever found in any of the Dip systems.

In July 1945, Cecil Phillips discovered the explanation for the early 1942 Trade usage which had long been thought to be some form of local reuse. It turned out that each cipher (key) page was used in normal fashion and then reused in reverse, digit by digit, if the message was longer than one page but shorter than three pages. Thus the odd pages of a message were enciphered in normal fashion and the even pages in reverse. This gave rise to about 4000 pages of a peculiar form of depth, all in the Red Code. From this came the sub-problem known as the Red Reverse problem, staffed by a dozen or more new people made available to the unit at the end of the war against Japan. These depths had no promise of intelligence production but would be very useful in the Venona exploitation.[33]

[31] Interview of Dr. Chew by Benson and Phillips, 5 August 1992, Washington D.C. Dr. Chew told us that he had taken the Army's correspondence course in cryptanalysis before the war (as had Gloria Forbes and many others). However, he was recruited by Dr. Leslie Rutledge, who had joined Arlington Hall during 1942. Chew, a member of an old Anne Arundel County, Maryland family, graduated from St. John's College, Annapolis in 1931, and received a PhD from Harvard in 1937. Chew, Rutledge, Captain Bill Smith (head of the Russian problem at this point in our narrative) and Lt. Ferdinand Coudert (his predecessor) had all known each other at Harvard. During the war years, Chew, Smith and Rutledge shared a large house in Washington on Newark Street.

[32] All of this is from the Phillips paper cited above.

[33] Phillips paper and recollections; Mr. Phillips used reports dated 15 April 1945 and 15 August 1945, held in his study materials, Venona collection.

In April 1945, the unit completed the machine processes of matching key digraphs to find Trade-Trade depths. This produced a large number of reused pages. But this technique gave way to the Hypothetical Additive Bank because of the latter's potential for finding more [redacted] or other non-Trade depths. The [redacted] success of November 1944, in finding depth by using the Hypothetical Additive Bank, had made this approach the primary method for depth finding. By August 1945, this method produced the first of the Canberra (Australia) KGB matches—ultimately an important depth.

Miss Jean Norris—a transfer from the weather section—joined Cecil Phillips, who had now taken full responsibility for machine liaison from Miss Dunning. They expanded the Hypothetical Additive Bank and began machine attacks on other problems. Phillips also picked up responsibility for [redacted] (GRU–naval) and [redacted] (GRU) during 1945. In August 1945, an attack was made on [redacted] (consular) without much success, though Dr Richard Leibler later built on it in the early 1950s and produced some text in conjunction with Meredith Gardner. The [redacted] effort involved isologs, generally circular messages in the same code using different additive pads.[34]

By the end of 1945, Arlington Hall had made an entry into a Russian machine cipher, known as [redacted] or Pink. Senior cryptanalysts Robert Ferner and Mary Jo Dunning collaborated to solve a bust in this system that had been found by Miss Doris Valley (a Cherokee from Oklahoma who was working in the traffic section logging and formatting [redacted] messages). This and some other potential breakthroughs against Russian military systems probably made the Russian Diplomatic problem—Venona—less interesting to Arlington Hall and its consumers, one of the many factors in the slow road to the Venona opening.

SAUTER

H. TICOM and BOURBON: US–UK Joint activities in 1945

Shortly before the end of World War II, the U.S. and the UK began to share the fact of and some details of their Russian Sigint programs and began planning for joint or complementary operations against that target. The codename for the overall Russian target became Rattan and later Bourbon.

The TICOM program (Target Intelligence Committee), established before Rattan/Bourbon, had as its objective the collection of German (and later Japanese) Sigint and Comsec information, records and equipment. It might be compared to the TAREX programs of later years. The TICOM teams found information about Russian systems in the German records and began sending this back to their respective Sigint centers, though with the understanding that GC&CS would be the central repository—actually Arlington Hall, Navy and GC&CS got a copy of everything.

In this section we will trace these two developments. At this stage it is still not possible, or at least not wise from an historical perspective, to completely separate the Venona project from the rest of the Russian program(s). At Arlington Hall, Captain Bill Smith's Russian unit still handled all Russian traffic—Dip, military and plaintext. As we have seen, the entire Russian program was compartmented.

TICOM, with its antecedents and descendants, is a very complicated subject, not least because the records [redacted] are difficult to use. Furthermore, the legends about the OSS and "the Russian codebook(s)" lead to considerable misunderstanding about our Venona breakthrough. It is probably useful to give the most important conclusions in advance, expanding on them in this and later sections as necessary. These conclusions:

1. The people who broke the KGB and GRU systems—Venona—have no recollection of seeing, hearing about, or using any Russian cryptographic material provided by the OSS. Meredith Gardner and Frank Rowlett

[34] Ibid.

were quite plain-spoken on this point. Likewise, Ferdinand Coudert, at the center of the Russian program before the Venona break (Spring 1943 til the end of 1945) said the Russian unit received nothing of interest from the OSS. The documentary evidence supports this.

2. The TICOM operation, conducted by US–UK military and naval personnel from the cryptologic and intelligence services, did acquire Russian cryptographic material of some importance to the Venona effort. But while that material assisted Meredith Gardner et al in bookbreaking, nothing could be done until the cipher (that is, the additive or key) had been stripped off the message groups to reveal true code groups. At that point, a codebook would be helpful. But, the greatest and earliest Venona break, into KGB system [redacted] was made without the benefit of any captured material that directly concerned that system. It was an immense analytic job involving dozens of people.

3. In the end, the TICOM effort assisted in the US–UK attack against Russian targets and was especially useful for its contribution to a general understanding of Russian systems, and, starting in 1953–54, for the entry into KGB system [redacted] (which had been in use before the [redacted] mentioned above).

September 1944 was a very busy month in the history of special support to Sigint operations against the Russian target —or we should say, potentially important. On 21 September, an advance party of the Finnish Sigint service arrived in Sweden with their records and equipment, an evacuation that had been coordinated with the Swedish services. Within a few days, U.S. State Department representatives began meeting with the Finns to learn about their attacks on U.S. crypto systems (in November, Lieutenant Paavo Carlson of Arlington Hall and Paul E. Goldsberry, a cryptographic officer from State, entered Sweden under diplomatic cover to continue debriefing the Finnish intelligence personnel). On 26 September the Drafting Subcommittee of the just formed Target Intelligence Committee (TICOM) held its first meeting.

As we have seen from the foreign cryptographic intelligence reported in Japanese Military Attache (JMA) communications, the Finns had an active Sigint operation. It had become clear from our reading of JMA that the Finns had been able to read some Russian and U.S. systems, and that they shared information with the Japanese and the Germans.[35] In the summer of 1944, the Finns realized they were on the wrong side and began negotiations with the Russians to save what they could. The Finnish intelligence services did not intend to stay around while the Russians installed a puppet government or occupied the country. The Finns had cooperated with the intelligence services of their neutral neighbor, Sweden, for many years. Major General Carl Ehrensvard, chief of the Swedish Defense Staff worked out an arrangement with Colonel Hallamaa of the Finnish intelligence services for the reception of Finnish personnel, along with their records and equipment. The first evacuees arrived in Sweden on 21 September. The Finns then assisted the Swedes in collection against both Germany and Russia.[36]

Eventually the Finnish Sigint group and its records, memories and equipment would be known as source Stella Polaris, and by the British, who later had some control over them, as Source 267. In some ways Stella Polaris/Source 267 and TICOM drew from the same fundamental source for information on, at least, Russian Dip, including KGB and GRU. It came about something like this. The Finns (presumably their security police)

[35] Finland, perhaps because it had paid its World War I debt to the U.S. and had waged a very heroic fight against the invading Russians in the war of 1939–40 (the Winter War), enjoyed a good reputation with the U.S. and UK. Colonel John Tiltman of GC&CS had established Sigint liaison with the Finns in 1940. But in order to recover lost territory, Finland made a secret alliance with Nazi Germany in 1941, and then joined the Germans in the invasion of Russia. Finland also allied itself with Japan becoming a partner in the Axis combination.

[36] [redacted]

had entered the Soviet consulate at Petsamo (Pechengo), Finland on or about 22 June 1941, when the Germans began their invasion of Russia. The Finns didn't join the invasion forces for several days but apparently the Russians went to emergency destruction and evacuation procedures right away. It is also possible that German forces (from the occupation forces in Norway) actually got into the consulate, as Germans staged through the Petsamo area. In any event the Russian destruction procedures were incomplete and the Finns grabbed what turned out to be a partially burned codebook of the First Chief Directorate of the KGB, that is the foreign intelligence element of the organization responsible for espionage and counterespionage abroad. This codebook (KOD POBJEDA), and its indicator system later came to be known as [redacted] The Petsamo trove also included KOD 26, a true Dip (consular) codebook, and at least one GRU codebook, as well as rules for using the one-time pads (the additive) to encipher groups from the codebooks, and instructions for using an emergency cipher system in case of compromise of the regular systems. The latter, known in the Venona world as the "Petsamo Emergency System", gave US–UK cryptanalysts an idea of how the Russians used these special hand systems, so important to agent operations.[37] Some traffic, plaintext and cipher text was also taken at Petsamo. Another important find, KOD 14, used by the NKVD rear service security troops, had been seized by the Finns during military operations on the Karelian front.

So, the Finns made a substantial haul at Petsamo and elsewhere. Photocopies went to the Germans, and probably the Japanese. The Swedes got their copies in 1944. This material formed an important asset of the Stella Polaris/Source 267 group. When the British took over this source in 1946, they too got copies of the Petsamo material and passed more copies along to the Arlington Hall. During 1946, the OSS successor/CIA predecessor organization, which (as the OSS) had infiltrated the Stella Polaris group starting in 1944 or 1945, also got some of this material. However, the real story is this: in 1945, TICOM had already obtained all of this and more in their sweep through the German Sigint centers, the teams seizing German photocopies of the material originally taken by the Finns (or maybe the Germans themselves) at Petsamo.

On 29 Sep 1944, L. Randolph Higgs of the US Embassy in Stockholm secretly met with the Finnish Colonel Hallamaa to learn about the apparent exploitability of our codes and ciphers, especially State Department systems. In a memorandum concerning that meeting Higgs wrote that, "(we) were most careful at all times to say nothing regarding any similar activities on the part of the United States, or to give away any information regarding our codes which Col. Hallamaa did not demonstrate beyond all doubt he already had." The Finn certainly gave Mr. Higgs an earful, and Higgs reported:[38]

> *They [the Finns] had been greatly aided in their work on breaking our strips by carelessness on our part in the preparation of messages; (for example) we were constantly putting information in ciphers they had already broken regarding messages in new ciphers, after which they could 'crack' the new ones.*
>
> *His general confidence in their ability to decode any of our messages anytime they wanted to, suggests very strongly that they do just that.*

[37] These systems might be based on a book or statistical chart or a remembered phrase. The agent and the Center would have the same edition of the book (perhaps a novel or travel book) and could construct keys and encipherment tables from them. Many Venona messages talk about systems of this sort, sometimes naming the book that agents in Mexico and South America will use in secret- writing letters or clandestine radio communications. The Petsamo Emergency System was for the consul, but the crypto procedure was the same for the KGB (who after all designed all crypto systems for all users).

[38] The Higgs memorandum, dated 30 September 1944 is in the CCH Collection. Hank Schorreck, Agency historian obtained a copy at the National Archives.

> *Most of their efforts, he pointed out, were naturally exerted on Soviet codes, of which he claimed they had broken over a thousand. He exhibited convincing specimens of their work on Soviet codes.*

One day in early November Colonel Harold Hayes, chief of Sigint operations at Arlington Hall, told Lt. Paavo Carlson (whose earlier personnel recruiting duties are described in Chapter II) to immediately report to the Pentagon for a meeting with Carter W. Clarke. At that time Carlson was working on the Finnish problem [redacted] for Mr. Arnold Dumey. Colonel Clarke told him he would be going to Stockholm to act as an interpreter. Clarke said that he would be met there by Colonel Raines, the U.S. Military Attache to Sweden and his assistant, Major Robert Wood, but Carlson was not to show that he already knew both of them. By coincidence, he had worked for them when they were, respectively, the G–2 and assistant G–2 at First Army Headquarters, Governor's Island.[39] Clarke then sent him to the State Department where he was given a new background identity, as a State Department employee who had graduated from the University of Alabama (rather than his actual school, Clemson). He retained his true name, however.[40]

The next day Carlson and State Department cryptographic expert Paul E. Goldsberry flew out of Andrews AFB, eventually reaching Stockholm after layovers in Iceland and Prestwick, where Count Bernadotte joined the flight.

Starting on 16 November 1944, Lt. Carlson and Paul E. Goldsberry began questioning Finnish Sigint personnel. In commenting on their report dated 23 November, Mr. Higgs of the U.S. Embassy made this important remark (he had been at the sessions too):

> *At no time did we receive any Russian code material nor did we ask for any from the Finns.*

The Carlson/Goldsberry report, which bears no letterhead or subject line (and no signatures, only initials) described in some detail how the Finns had exploited U.S. Dip systems and that they and the Germans were exploiting many other Allied and Neutral systems too. The Finns denied that they had given anything to the Japanese! Carlson and Goldsberry summarized some of the comments the Finns made about their work on Russian systems:

> *Russian diplomatic codes are unbreakable—said they used a block of cipher groups and enciphered plain text only once on each group.*
>
> *Captain Palle [a Finnish officer] stated that collaboration with Germany consisted of exchange of information regarding Russia. Just enough to be an ally. Stated you have to 'give a little and take a little'.*
>
> *Entire (Finnish) organization 1000–1200 people of which greater part worked on Russian military and naval codes with such success that they were able to break a new code within two weeks after its first appearance.*

[39] Major Wood, a West Point graduate, was the son of General Robert Wood, the CEO of Sears, Roebuck. He had left the Army during the Depression to free up a Regular officer slot for the Army, which was then going through a reduction. Colonel Al McCormack was presumably referring to Colonel Raines when he mentioned having told the G–2 at Governor's Island (Ft. Jay) about the Coudert Commission records concerning communist activities in New York. Ferdinand Coudert, of the [redacted] problem was the brother of that (then state senator and later U.S. representative) Coudert.

[40] Clemson was an all male military college at that time—perhaps the University of Alabama gave better civilian cover while yet being a Southern school. Carlson had been commissioned through ROTC at Clemson. He was working as an insurance agent in New York City when called to active duty in June 1941. Carlson had been born in the Finnish neighborhood of New York City and spoke the language.

> *He broached the subject of some of their experts going to the United States where their analytical ability could be put to use.*[41]

Interestingly enough, Paavo Carlson's most vivid memory of these meetings concerned German, not Russian, material. He recalled how OSS officer Wilho Tikander opened a suitcase filled with U.S. currency and handed it over to the Finns, in exchange for a German Enigma machine with the wheels.[42]

The Stella Polaris (Finnish) group continued to make overtures to the British and Americans during the last year of the war, eventually becoming, as stated, the British Source 267 re-located to Paris. Apparently they did indeed, as the legend has it, sell Russian codebooks to the OSS.[43] In January 1945, the Swedes returned to the Russian controlled government of Finland some of the material that had been brought out by the Finnish Sigint Service. Nothing of import was returned, unless it had first been copied. The OSS view of the Stella Polaris group was that:

> *On the basis of the record and of inside information which indicated more or less complete penetration of the Finnish resistance—and of Stella Polaris itself—by Soviet and Soviet-controlled Finnish agents, [OSS] rejected these overtures and restricted itself to the counter-espionage coverage and limited positive intelligence exploitation of the group's facilities through our own agents within it.*[44]

In a memo of 11 Oct 1946, the Army G–2 gave the Director of Central Intelligence an appraisal of the Stella Polaris/Source 267 material and some background, concluding that most of the material had already become available through TICOM—but that it was well to keep this emigre Finnish Sigint group occupied lest they sell out to another party.[45]

One final note on the OSS and Russian material. We know that General William Donovan, chief of the OSS, with the approval of President Roosevelt, entered into negotiations and an exchange agreement with the KGB concerning operations against Nazi Germany. According to General Deane, the head of the U.S. military mission to Moscow, who acted as Donovan's liaison to the KGB, the OSS gave the Russians a considerable amount of information (and of course got little in return) including some documentary proof that the Germans had broken certain Russian codes (which seems to be a separate episode from the November 1944 purchases

[41] Hank Schorreck also obtained a copy of this memo from the National Archives.

[42] In our interview, Mr. Carlson had no recollection of the discussion with the Finns about Russian cryptography. He believed that the sessions he attended were unilateral—that is the Swedish services were not present. Tikander and Colonel Raines seemed to be in charge. Carlson noted, however, that he was under surveillance and his hotel room searched, presumably by the Swedish security police. (However, he did identify his initials on the aforementioned report).

[43] See The Shadow Warriors, by Bradley F. Smith (Basic Books, New York, 1983). I have not looked at Smith's sources or otherwise examined OSS records (other than those held by NSA). Briefly, Smith's story is this: "In November 1944, OSS Stockholm was offered an opportunity to buy from Finnish sources numerous Soviet military documents . . . in early December, OSS Stockholm purchased 1500 pages of Soviet material and the code keys from Finnish representatives." And, "On 11 December, Donovan reported to Roosevelt that he had purchased one military and three diplomatic codes and turned them over to the State and War Departments." This cryptographic material was ultimately returned to the Russians on orders of Secretary of State Stettinius. We will discuss some of this again in the chapter on KGB/GRU penetration of the OSS. We have, of course, no record of any Russian material acquired by the OSS ever reaching the War Department.

[44] Memorandum for the Director of Intelligence, the Pentagon (i.e., G–2) from the Central Intelligence Group, 4 November 1946. NSA Archives CBRJ 23 [redacted] The CIG followed OSS and would soon become the CIA.

[45] Ibid.

EXEMPT

in Stockholm for which see footnote 40). This affair remains murky even today, and we cannot be certain just what crypt material Donovan showed the KGB.[46]

The TICOM came into existence under the auspices of the Chiefs of Staff of the US and UK. Mr. F.H. (later Professor) Hinsley of GC&CS often chaired meetings of the committee.[47] Colonel George Bicher, an Arlington Hall veteran, and General Eisenhower's senior Sigint officer in the European Theater, was the senior U.S. representative. The purpose of TICOM, as mentioned earlier, was the recovery and study of German Sigint and cryptographic materials—to seize important records and equipment, destroy what could not be taken, destroy German Sigint capability, detain and interrogate key German cryptologic personnel. To do all this, the US and UK formed TICOM teams composed of military and naval intelligence people who were to receive support from local commanders. Some of the early plans of the committee now seem a bit fanciful, for example, the plan to use five U.S. Army infantry battalions to seize German cryptologic centers in Berlin.

Eventually, some six joint TICOM teams were established. The team composition, and team numbers changed from time to time, which occasionally makes it difficult to sort out who was doing what. Some well known NSA people were on those teams, including (with their 1944/45 ranks): Lt. Oliver Kirby, Lt. Arthur J. Levenson, T/3 Arthur Lewis, Lt. James K. Lively, Lt. Selmer Norland, T/Sgt George Vergine and Lt.Col. Paul E. Neff; also Major William P. Bundy of that family famous in higher government circles.

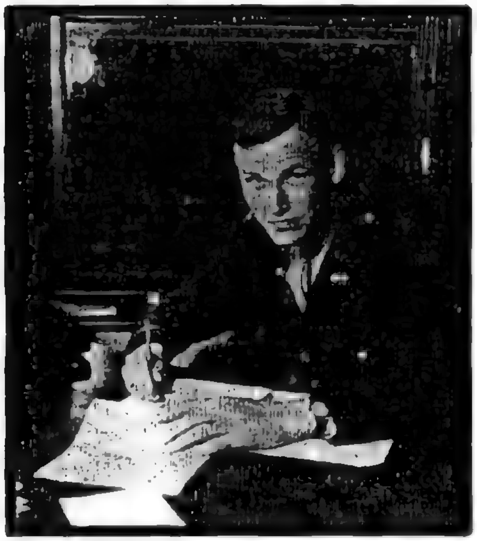
Team 3, previously known as Team 5, under the command of Lt. Col Paul Neff, assisted by Lt. Col. Geoffrey H. Evans, Intelligence Corps, British Army, found the Russian material of greatest interest to the Venona story. Other members of that team included Major Bundy, Captain Duncan McIntyre, Major R.W. Adams, Sergeants F.A. Marx, and I. Loram, and Cpl. Schnabel, all of the U.S. Army (all ETOUSA Sigint people). Major Caddick acted as a courier and Lt. Stribling coordinated transportation. Some others probably were on the team.[48]

[46] See Deane's Strange Alliance. Deane gives an extraordinary and vivid account of his and Donovan's meetings in Moscow with General Fitin, head of the First Chief Directorate of the KGB (the foreign intelligence directorate). Fitin, covername Viktor, directed the KGB operations against the U.S. One of Fitin's many agents inside the OSS was Major Duncan Lee, Donovan's executive assistant.

[47] Professor Hinsley is principal author of the multi-volume Official History of British Intelligence during the Second World War.

[48] See TICOM/I.1, Final Report of TICOM TEAM 3, 8 June 1945. Lt Col Evans, British Army, probably wrote the report. Mr. Lou Maddison, GCHQ archivist and Venona expert, often cited in this study, told me that Team 3 made the big Russian finds. Happily, Lou gave me an extra copy of this report, because I have not been able to find a copy in NSA records.

LtCol Paul Neff receives the Legion of Merit, July 1945. He headed TICOM Team 3 in the Burg Operation.



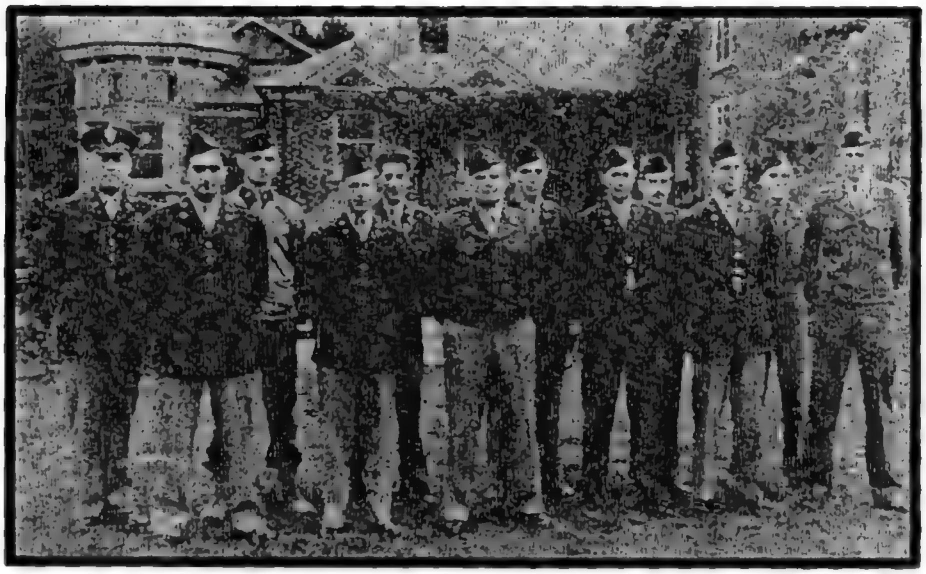
Major William P. Bundy, member of TICOM Team 3.

On about 18 April 1945, Lt. Alfred G. Fenn, Provisional Detachment 14, Provisional Government element, First U.S. Army, visited the castle at Burgscheidungen, hereafter Burg, near Naumberg, Saxony–Anhalt in east-central Germany, an area that was about to be turned over to the Russians according to the agreement on Allied zones (the war continued for about 2 weeks after this date). He spoke to the owner of the castle, with Miss Friedrichs and Mr. Rohrbach of the German Foreign Office present to assist in the conversations. Friedrichs, was reluctant to discuss the official duties that she had been carrying out at the castle. Lt. Fenn returned a few days later to demand more information and learned that Friedrichs and Rohrbach had been with a cryptologic unit of the German Foreign Office working at the castle. Fenn obtained basic information about their work and the records, and then warned them that they would be executed if the files were disturbed prior to U.S. inspection. Lt. Fenn's information about Burg reached Colonel Cleaves, Signal Officer V Corps. Cleaves telephoned Colonel Bicher. A guard detachment from the 102nd Cavalry Regiment then secured the castle.

TICOM Team 3 left Paris in automobiles on 25 April, driving to Burg via Verdun, Wiesbaden, Weimar and Naumburg, reaching the castle on 27 April. They found that Burg had been a principal cryptanalytic center for the Sigint element of the German Foreign Office, with records intact and key personnel waiting around to be questioned—undoubtedly relieved that the Americans and British had gotten there before the Russians. The team worked at the castle and nearby Sigint-related facilities for two weeks, inventorying the material, packing it and questioning the Germans. Security was particularly important, because the Russians were expected to arrive soon. Lt Col Neff arranged the evacuation, to Marburg in the American zone, of all Germans who might have been in contact with the team in the Burg area. Equipment, records and people were flown out of a nearby airfield on 7 May, on 9 May a truck convoy took out the rest of the people and material. On VE Day (8 May) engineers from the U.S. 104th Infantry Division blew up the German machine processing equipment.

The Neff/Evans team shipped the contents of 73 steel file cabinets. The Burg cache included 300,000 pages of material. Major John Seaman, Arlington Hall's chief representative to GC&CS, advised headquarters that the haul included "some 'Bill Smith' material". Smith was at that time still heading the Russian problem.[49] Some of the team's material, shipped to GC&CS for study, was microfilmed and sent on to Arlington Hall rather quickly. In one of the messages concerning the Burg material we read, "Seaman is sending much 'Bill Smith' material"; in another message Smith asks Seaman to microfilm material of interest to him, and in a 25 June report we learn that Arlington Hall had received "further material for Bill Smith", probably picked up by Oliver Kirby two weeks earlier.[50]

[49] TICOMMA Report, 11 June 1945 in the NSA Archives, CBQK 76 in a folder of TICOMMA reports for 1945 and 1946 (TICOMMA meant TICOM Admin reports?)
[50] See the aforementioned TICOMMA folder.



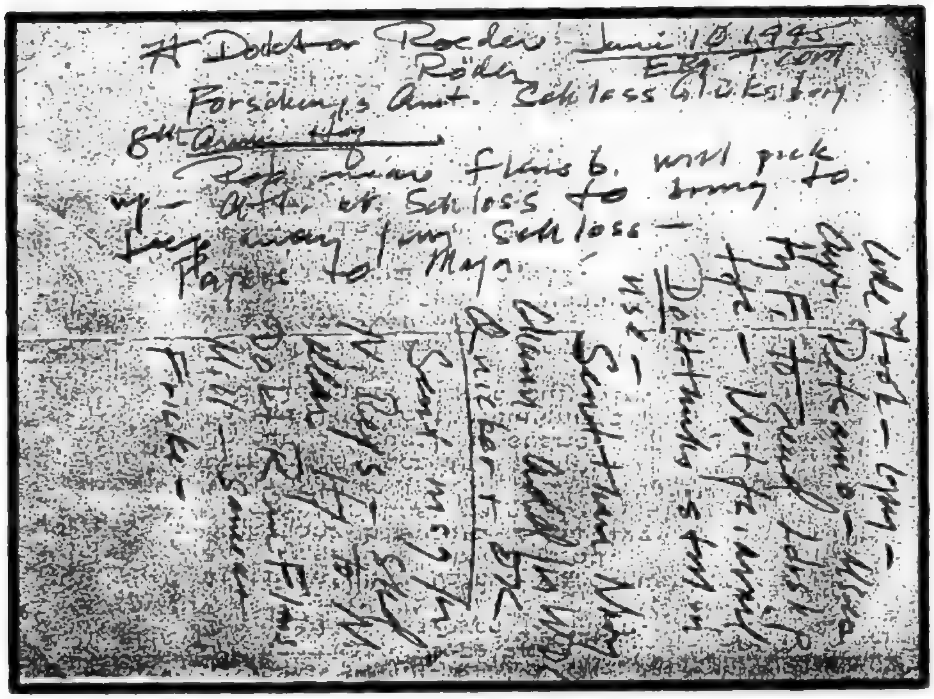
Army Sigint officers in UK, 1943. Oliver Kirby (5th from right), Bill Bundy (far right) and Arthur Levenson (5th from left).

On 10 June 1945, Lt. Oliver Kirby, a U.S. Army Sigint officer, temporarily serving with British Naval Intelligence detachment 12 A/TICOM Team 6, discovered more Russian cryptographic material.[51] Kirby had been commissioned through ROTC upon his graduation from the University of Illinois.[52] In 1943 he went to the UK as part of the 6813th Signal Security Detachment (Provisional), an Arlington Hall field operating unit that had been formed to give the U.S. a greater role in working German Enigma traffic.[53] Most Army personnel detailed to the TICOM teams came from that unit. One of Kirby's TICOM assignments was to interrogate a Dr. Roeder who had been a member of the German Foreign Office Cryptanalytic organization that Lt. Colonel Neff's team had exploited. Roeder was being held at Schloss Glucksberg in Schleswig, near the old Danish town of Flensburg. Mr. Kirby has preserved his notes from that meeting (which he made on the back of a poem written by a British officer):

[51] Commander Alexander M.S. Mackenzie, R.N.V.R., headed Team 6. Information in this section from interview of Oliver Kirby, in Dallas, Texas, 1 March 1993.

[52] Most of the officers arriving at Arlington Hall in 1942 were reservists who had been commissioned through ROTC. A number of officers, e.g. Ferdinand Coudert received commissions direct from civilian life. By 1943 the Signal Corps Officer Candidate School (OCS) provided most officers for the Signal Security Agency. Very few regular officers served at Arlington Hall or at its field locations.

[53] The organizational history of Army Sigint in the European Theater is most complex. Colonel George Bicher, an Arlington Hall veteran, was the senior cryptologic officer in the European Theater of Operations from 1942–1945. He commanded the Signal Intelligence Division, European Theater of Operations, U.S. Army (SID ETOUSA), with headquarters at 59 Weymouth Street in London. SID–ETOUSA was at once a staff, operational, technical and training organization. It had a field processing element with extensive communications links within the UK, to Arlington Hall and to the Sigint units that went into France in June 1944. Various tactical intercept companies, until deployed to the continent, came under SID–ETOUSA. The 6913th, aimed against higher echelon German communications, also came under Colonel Bicher, as did the U.S. TICOM personnel. The 6913th was housed at Little Brick Hill, near Bletchley Park.



Oliver Kirby's notes upon recovering Russian Dip codecook, near Flensburg, 10 June 1945.

H. Doktor Roeder Juni 10 1945
Near Flesb., will pick up . . . At Schloss, to bring away from Schloss. Papers to Major.

Code Book - copy - captured Petsamo. Used by [Germans] to read Ldrshp tfc. No tfc. avail. Dokt. thinks still in use.

Sent thru Navy channels. Add. for WDC. Quicker and OK. Sent msg. for N. Reps. Dokt. R. in Flns. Mill—same as Fricke.

Kirby had found a photocopy of Code 26, the Russian consular codebook taken at Petsamo in 1941. Note Dr. Roeder's claim that the Germans read this diplomatic system. This seems unlikely unless the Germans had key pads or had successfully worked Code 26 material enciphered in other than one time pad (such as the Emergency System). Kirby put the material in approved Navy channels and it was flown back to the U.S., probably via London.[54]

In later reports from Major Seaman and his successor Captain C.P. Collins we see the TICOM inventory numbers that had been assigned to the material and can therefore identify items that were later used for the Venona exploitation, T–1014 and T–1015 were, respectively, the GRU (naval) codebook and the KGB codebook for system [redacted] Seaman describes these as "System TB Petsamo 1941" material and as

[54] Lt. Kirby had other special missions during that time. In one, he and a Royal Marine driver who spoke some Russian crossed into the Russian lines at Minden, under a suitable pretext, to look for German atomic energy records that reportedly had been thrown down a well. In a second mission he went to Flensburg to look for a German who had been involved in burst communications. As he drove up to the meeting place at the harbor, a group of naval mines broke loose from storage racks, collided and exploded causing many casualties. He was blown from his jeep and did not meet the burst expert until 20 years later at a conference with the Third Party. He did however track down the designer of the Goliath VLF U–boat communications system—in a field near Kiel where the man was cutting peat. Kirby told me that the Royal Marines' Amphibious Assault Unit (AAU) supported him in all these activities.

EXEMPT

"charred fragments of Russian 4/F Dipl codebook".[55] He and Collins also mention the filming of T–961 and T–3355 (actually identical items) which were later identified as KOD 14, used by the NKVD rear area troops, and TICOM 1 to 7, 9–11 and 14. TICOM 10, apparently included in the foregoing was KOD 26, the consular code only partially burned in the evacuation of Petsamo.[56]

It is this material, mostly recovered by TICOM Team 3, and by Lt. Kirby, that has been the basis for many Venona legends, such as that the breakthrough came about because of a charred Russian codebook recovered from the battlefield, by the OSS or by the Finns and given or sold to the OSS and etc.[57] Some of the material is charred and the circumstances of the recovery are indeed interesting, but for battlefield we have to substitute a classified trash fire at the Soviet Consulate in Petsamo and a collection at a castle in eastern Germany, and for OSS read TICOM Team 3, Oliver Kirby (and the Finns, Stella Polaris/Source 267). Meredith Gardner, who was the first person to recognize the KGB nature of [redacted] later told Bob Lamphere of the FBI that the codebook that he (Gardner) used to make the breakthrough had been found on a battlefield and had a bullethole in it. Meredith later told me that he was referring to a mark that looked like a bullethole but certainly wasn't. We are getting ahead of the story, but the book that Meredith was using was the aforementioned KOD 14, which he studied to learn possible KGB codebook vocabulary and just to see what a Russian codebook looked like. It was not a Venona system, and did not lead to the first Venona break, which was accomplished by bookbreaking without the benefit of the relevant book [redacted] Pages 86 and 87 of the KOD 14 book (which I've only seen in photocopy) do indeed show a round, but irregular, black mark—probably an ink blot.

Soon after the TICOM teams had been deployed to the field, the U.S. and UK made arrangements to cooperate on the Russian problem. The U.S. used this development to further the process of Army–Navy Sigint consolidation that finally led to the creation of AFSA and then NSA. In July 1945, Captain Joseph Wenger of OP–20–G and General Preston Corderman, head of the Arlington Hall operation (soon to change its organizational name from Signal Security Agency, SSA to the Army Security Agency, ASA) agreed that liaison with the British on Rattan, the codename for the Russian problem, would be under the auspices of the joint Army–Navy Communications Intelligence Coordinating Committee (ANCICC) rather than individually be each service.[58]

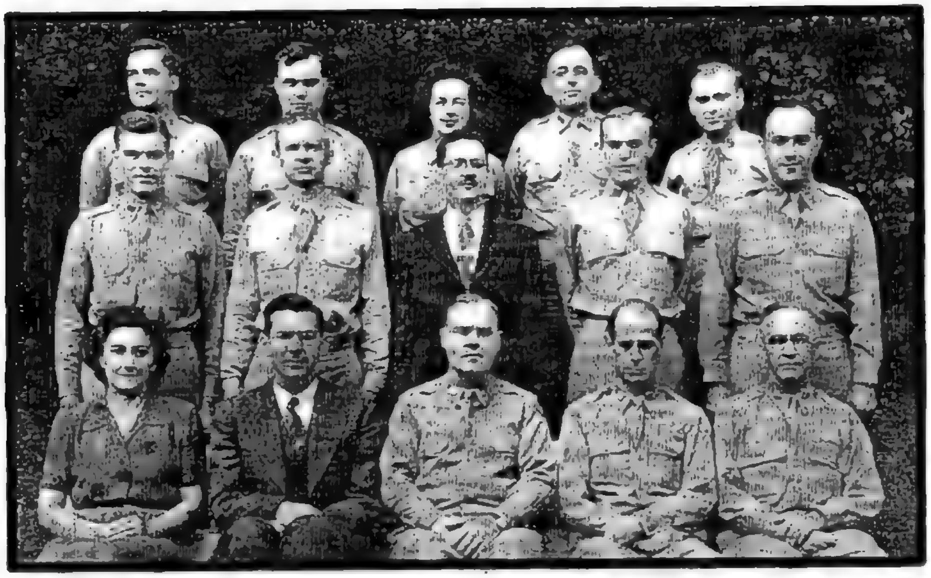
EXEMPT

[55] Memo Seaman to CG SSA, 17 July 1945 in NSA Archives, CBQK 47.

[56] The Seaman and Collins reports are in the NSA Archives at Ibid.

[57] *The Final Report of TICOM Team 3 does not specify what documents were found at Burg. Mr. Lou Maddison, GCHQ archivist, told me that Team 3 made the major finds, including a copy of KOD PODJEDA and the other Petsamo items.*

[58] Memo Wenger to OP–20, 16 July 1945. NSA Archives at CBQM36 in folders "Bourbon Semi-Monthly Reports and Related Documents". Except as otherwise noted, my brief summary of Bourbon is based on that collection of papers and no further citation will be made. Both the NSA Archives and the CCH Collection have other groups of documents on this subject.



LtCol Frank Rowlett with staff, 1945. Bill Smith (top row, 2nd from right) and Maurice Klein (far right 2nd row).

British and American cooperation on the Russian problem developed very quickly as outlined below in a series of quotes and extracts from ANCICC (later called STANCICC, with State Department added to Army and Navy) Bourbon progress reports. One interesting US–UK policy item, before we catalog the Bourbon evolution: it became apparent early on that the U.S. would no longer conceal from the British its work on Russian Dip and would willingly share not only "fact of" but also technical details. Edward Christopher and later Cecil Phillips would be sent to the UK to further this process. But once Arlington Hall discovered what was in the traffic—that it was not Dip but espionage traffic—a U.S. eyes-only policy would again be imposed, though briefly and probably not very effectively. A story for later sections of this study.

The Bourbon highlights:

- 7 Aug 1945. Major Seaman authorized to open negotiations with the British — first step to negotiate for immediate complete exchange of traffic, status of solutions, technical materials, techniques. Seaman to suggest to British that the codeword Bourbon replace Rattan.

- Seaman had learned on 5 Aug that British had only 3 or 4 months worth of Russian Dip traffic; no cable traffic to/from London but collection would begin.

- 8 Aug 1945. Washington to send Major Seaman additional information on Russian Dip systems with proposal that US–UK exchange back traffic on microfilm.

- 15 Aug 1945. Arlington Hall and Navy have identified 35 Russian systems, of these 6 were Dip and 2 of these in process of solution: depth of overlaps limited to two. TICOM has made clear that Russians use one time pads to encipher codes. Other than Dip, all US intercept from Russian Far Eastern nets.

- 15 Aug 1945. Sir Edward Travis, head of GCHQ "has confirmed our proposal that cooperation on Bourbon is to be complete, though informal". Travis has given Major Seaman access to all UK Bourbon material.

- Sep 1945. Discussion of further exchange of liaison officers.
- 16 Oct 1945. US liaison officers touring all British field stations.
- 16 Nov 1945. Captain C.P. Collins to relieve Major Seaman and Mr. Ed Christopher to relieve Mr Frank Lewis for Bourbon liaison at GCHQ.
- 1 Jan 1946. Arrangements for exchanging all Bourbon translations including back material.
- 16 Mar 1946. US begins receiving films of Source 267 material.
- Throughout this period, much discussion of Russian machine ciphers (military/NKVD)
- 27 June 1946. Bourbon liaison has been removed from special category, that is, the general Russian Sigint problem no longer a special compartment — Venona soon would be compartmented.

In the midst of all this, "C" wired the GCHQ representatives in the US as Immediate, 23 Sep 1945:

> *R.C.M.P. have in custody a cypher clerk from office of Soviet Military Attache. He has already provided some useful crypto information.*
>
> *Canadians have agreed, at our request, that he should be interrogated at once by American officer, if Americans will consent. We consider his information will probably be of considerable assistance if he is interrogated on technical matters by an officer fully versed in crypto problem involved.*
>
> *If Americans agree to send an officer (and Canadians ask that it be restricted to one only), please arrange that he contacts Stephenson in New York who will hand him over to appropriate contact in Canada. This is necessary to avoid crossing lines with FBI. Stephenson is steering FBI interrogations in Canada clear of crypto matters.*

A follow-up message the same day gave some crypt intelligence that the defector had provided in preliminary debriefings. The message specified that the point of contact for the U.S. would be Sir William Stephenson, head of British Secret Service operations in the Western Hemisphere 1940–45 (sometimes referred to as "Intrepid").

The ANCICC learned the next day from Group Captain Jones, a GCHQ liaison officer, of the foregoing. "After clearance from 20–G, Cominch, and G–2 was obtained, it was agreed that it might be profitable and not too dangerous to take advantage of the opportunity to have an Army officer interrogate the clerk."[59] Lt. Colonel Frank B. Rowlett departed Washington, in civilian clothes, on 25 September 1945, to question Lt. Igor Gouzenko, the GRU code clerk who had defected. The KGB almost caught Gouzenko, and after he got away KGB officers using crowbars broke into his apartment, but were turned away by the police. As we would later learn in the eventual decryption of one of the most famous Venona messages, Kim Philby had alerted KGB London upon learning of a message from Stephenson to "C" announcing the defection.

I. Gouzenko, Bentley, Chambers and the Anonymous Letter

A stunning series of closely spaced counterintelligence events took place in 1945: on 10 May the FBI had conducted a serious, all-day interrogation of Whittaker Chambers at his Time magazine office (Chambers earlier attempts to tell all had gone astray in the hands of A.A. Berle and Director Hoover); Gouzenko of the GRU defected in September; Elizabeth Bentley, a veteran KGB officer, gave the FBI a 107 page statement in

[59] From the collection of Bourbon papers cited above.

November. And for the past two years the FBI had been studying an anonymous letter, from a KGB (or just possibly GRU) officer. An incredible amount of information became available on Soviet espionage in the United States—but with very little documentation to back it up. Whittaker Chambers had saved a few papers that would help convict Alger Hiss; Gouzenko had a lot of papers on Canadian, but not American spies; Bentley, with the most to tell, had only her recollections. Venona would eventually provide the missing documentation and identify many more spies.

Frank Rowlett spent several days questioning Igor Gouzenko, codenamed "Corby", and the following paragraphs are based on his "Special Report on Bourbon Cryptography: Report on Interrogation of Corby", dated 15 October 1945.[60]

Rowlett learned that Gouzenko had gone to the RCMP o/a 10 Sep 1945, in fear of being called back to the Soviet Union because he had committed a serious security violation. He had first tried to go to Canadian newspapers with his story of Russian espionage but had been turned away (Russian trade official Kravchenko had "defected" to the New York press in 1944, reasoning that by going public he would be protected. We will see in Venona how the KGB and their American agents tried to track him down.) He then tried the Justice Ministry but was again rebuffed. Finally, the RCMP took him into protective custody (along with his pregnant wife and young son).

Rowlett drove to an isolated, lakeside summer cabin some 90 miles from Ottawa where Gouzenko was under guard. The Rowlett party included Professor Gilbert Robinson, a wartime Canadian Sigint officer, Inspector Leopold of the RCMP and a driver. (Robinson had conducted the preliminary questioning of Gouzenko on cryptologic matters— Gouzenko had given names of spies and supporting papers to the Secret Service, RCMP and FBI.) Rowlett learned that Russian cryptography, in the external affairs area, could be divided into two types:

- Systems used by Russian establishments abroad in communication with Moscow. These systems were entirely by encipherment of a code by a one-time additive.
- Emergency or illicit systems which used a substitution alphabet based on one and two-digit equivalents for the Cyrillic alphabet, which would then be enciphered by a one-time key generated from a book or other publication readily accessible to both Moscow and the communicant in the field, i.e., both Moscow and the field had to have the same book, same edition.

Gouzenko explained Russian crypto-security doctrine and procedures, and the day to day work of a GRU code clerk. All code clerks were approved and trained by the KGB. Every Russian official authorized to sign messages—the GRU Resident/Military or Naval Attache, the Trade Representative, the Ambassador or Consul had a code clerk assigned to him who would prepare the messages. These clerks were responsible to the KGB for security and procedures—the officials who drafted the messages could not keep file copies of the original texts of the messages they were releasing. In the case of the GRU Resident in Ottawa, he would bring his notes into the office of the code clerk, and in the presence of the code clerk write out a message. The code clerk, after the drafter had left the office, would encode the message and then take it to the mission's communications officer who would give it an external serial number and take it to the commercial cable company for transmission to Moscow (the Russian establishment in Ottawa did not at that time have its own communications facilities).

[60] Copies in the Venona Collection, but also in the NSA Archives at CBQM36.

The Russian text of a GRU message would be encoded by a four-digit, one-part code, that is, the code book was arranged in strict alphabetic order. When an item had to be put in the message for which no equivalent appeared in the code book, it was spelled out by means of a Cyrillic or Roman substitution alphabet which was issued as a supplementary chart to the code. When this chart was to be used the four-digit group 7810 would be entered, meaning "begin spell" and the end of the spelling would use a special two digit group, 91, to mean end of the spelling.

The GRU code text would then be enciphered by a one-time pad. All pads, for every agency of the Soviet government, were manufactured by the KGB. The pads had either 35 or 50 pages each and each page would contain ten lines of five 5–digit groups, for a total of 50 groups or 250 digits per page of pad. Each page or sheet of the pad had a two digit number in the upper left hand corner ranging from 01 to 35 or 50 depending on the number of pages in the pad. These pads were carefully packaged and controlled. When the message reached Moscow, a senior officer would determine the addressee and pass it to the appropriate code clerk. Gouzenko reported, curiously, that copies of these GRU messages would go directly to the KGB for analysis (perhaps he meant, also to the KGB). Gouzenko described for Rowlett, at some length, the emergency or illicit systems.

Gouzenko believed that the KGB, in producing all one time pads for the government, mechanically generated them using an apparatus, "which selects numbers purportedly at random by a device using small balls in some fashion. This apparatus was credited to the British originally, but certain improvements were made by the (KGB) cryptographers when it was adopted by them. No further information regarding pad generation is available."[61]

Rowlett concluded his report with a general observations section:

- While the KGB carefully screened candidates for work in the cryptanalytic organizations, the "standards are not so high as those set for cryptographers".
- A code clerk underwent 9 months of training.
- A code clerk was expected to have familiarity with the language of the country of assignment and be able to evaluate open source publications of that country.
- During the war, the Russians had considered the German one-time pad Dip systems as invulnerable as their own. (note by rlb: late in the war, Arlington Hall broke into the German one-time pad system, which undoubtedly led to optimism about eventual success against Russian Dip too).

A small team in Bill Smith's Russian unit consisting of Mrs. Genevieve Feinstein, Miss Mary Jo Dunning and Mr. Burton Phillips immediately began a study of the Rowlett report in context of the traffic on hand. It is maddening for the non-cryptanalyst to try to understand, but then to realize, that even with such a source as Gouzenko, who brought out plaintext of some of the GRU encrypted messages and explained the system in great and accurate detail, the traffic remained unbreakable. Gouzenko's background information on the Russian systems was certainly very important and helpful—but with it Arlington Hall could not read any traffic and could at best only add some words to book breaking vocabulary of the GRU code book. But the code book would not do anything unless the cipher additive, from the one time pads, could be identified and stripped off to reveal the underlying code groups. Gouzenko had no pads, and if he had it would only have given an opening into the message(s) enciphered by that particular pad. Gouzenko's most enduring contribution to Venona was to put the

[61] Throughout this account I stick very closely to Rowlett's words—putting it all in quotes seemed too tedious and I have done some editing anyway.

cryptanalyst into the office of a Russian code clerk, giving us an understanding of how he worked, and what his systems looked like and how they were used.

Whittaker Chambers and Elizabeth Bentley gave the names of KGB and GRU agents in the U.S., more than a year before the first Venona translation. A quick summary of their information is useful to the story of Venona and its place in U.S. counterintelligence history.

Whittaker Chambers

Chambers, a sometime editor of Time magazine, described a GRU network in Washington in the mid–1930s and reported to the FBI that Alger Hiss and Harry White had been members of the group, passing along classified information to the Russians. By 1945, when the FBI interviewed Chambers in detail, Hiss had become an important State Department official and Harry White an Assistant Secretary of the Treasury. Chambers provided enough documentary evidence to eventually convict Hiss of perjury. White, never charged, was still under investigation by the FBI when he died. Chambers could give no significant information about Russian espionage in the U.S. after about 1938 when he severed his Communist Party connections.

Elizabeth Bentley (left) and Alger Hiss (right) at Congressional hearing.

Elizabeth Bentley, a graduate of Vassar and Columbia with various employments over the years, may also have had a GRU connection during the later 1930s, but seems to have signed on with the KGB in 1940, acting under instructions of Jacob Golos, a KGB agent-officer in New York City and major net controller. Bentley served as courier between Washington and New York and sometime agent handler. She gradually lost interest in the work after Golos, her lover, died in November 1943—but it was two years before she ended all contact with the KGB and went to the FBI. In her long statement to the Bureau, Miss Bentley named almost 100 Americans and Russians connected to espionage or Communist Party activities in the U.S. Of the Americans, 51 were investigated by the FBI (27 of these held U.S. government positions as of the date Bentley went to the FBI). In terms of Venona, Bentley's information undoubtedly helped identify covernames in the traffic; she herself appears in the Venona decrypts seven times under the covername UMNITsA (Good Girl) during 1943 and 1944 and seven more times under the covername MIRNA during 1944—in fact some of the most interesting KGB tradecraft and security policy information in Venona concerns her. She told the FBI that Harry White was working for the KGB, as was Major Duncan Lee, sometime executive officer to General Donovan, head of the OSS. She described the agent net run by Gregory Silvermaster, a government employee, and named the people under his control. As we have seen, she told the FBI that the KGB had learned something about Arlington Hall's Russian Sigint program. Some 29 Americans identified by her as having connections to the KGB appear in the Venona traffic. Undoubtedly many more are in Venona as unidentified or unrecovered covernames. Venona identified more spies, in nets with which she was not involved. We can state quite confidently that the controversial information she provided, first to the FBI and later to a grand jury, to Congress and to the public, was accurate. Unfortunately, most of the information she gave would be insufficient for prosecution. She brought out no papers and no one (almost no one at least) provided any corroboration.

While it is generally believed that the Gouzenko-Chambers-Bentley revelations of 1945, were the first real break into Soviet espionage in North America, one more source needs to be mentioned: the Anonymous Letter of 1943. Written in Russian and addressed to FBI Director Hoover, the unsigned and undated letter was postmarked Washington,D.C., 2 a.m., 7 August 1943. The writer has never been identified but was presumably a KGB (or possibly GRU) officer assigned to Washington. This strange document named only two American agents of the KGB, but identified major officers of the New York, Washington and San Francisco Residencies—once again, names that would figure prominently (under covernames) in Venona.[62] The writer said he was coming forward because KGB officers in the U.S. were in the pay of Japan! This absurd statement may have been made because the author feared his information on Russian espionage in the U.S. would be ignored unless it was somehow connected to the Axis. Some highlights of the letter (which appears in full in an appendix):

- U.S. Communist Party leader Earl Browder was a KGB agent.
- The KGB chief in the U.S. was Vasili Zubilin (true name Zarubin), assisted by his wife, also a KGB officer.
- Zubilin's principal assistants included Pavel Klaren, vice-consul in New York; Khejfets, vice-consul in San Francisco; Kvasnikov, the technical intelligence chief; Shevchenko, operating in Buffalo under Purchasing Commission cover; Mironov (true name Markov) and more.

[62] The Anonymous Letter named Boris Morros of Hollywood and C.P. Chairman Earl Browder as KGB agents.

- Zubilin, a KGB general, had directed NKVD police and troop work in the occupation of eastern Poland in 1939, and with Mironov, had been in charge of the murder of the 10,000 Polish officer prisoners thereafter (the reference here is to the Katyn Massacres of 1940).

All of this information was true and much elaborated upon in Venona, e.g., Khejfets the KGB Resident in San Francisco; Kvasnikov running the atomic bomb espionage operation. We probably see reflections in Venona of the FBI investigation into the leads provided in this letter, for example the KGB in New York and San Francisco reporting to the Center about increased FBI surveillance activities; Zubilin complaining to Moscow that his activities in Poland have apparently become known.[63]

[63] See Appendix Two of this study for the text. Copies of The Anonymous Letter are in the Venona collection in box D046, 54–001 and elsewhere. Arlington Hall seems to have gotten its first copy of this letter in about 1949. Meredith Gardner made a translation of it, that is, he did another version to add to the original FBI translation. Bob Lamphere told me that the Bureau made a tremendous but unsuccessful effort to identify the writer—one can only wonder what would have happened if the writer could have been grabbed and turned (or simply taken in as a defector). This letter is of considerable historical importance and raises many questions about U.S. counterintelligence during the war.